Web Seminar BPKP

Pemanfaatan Teknologi Digital dan Proses Analisis Bukti Digital

Selasa, 27 Oktober 2020
Pusat Pendidikan dan Pelatihan Pengawasan BPKP

Yudi Prayudi
Pusat Studi Forensika Digital
Universitas Islam Indonesia

Profile

Yudi Prayudi

S1 UGM : Computer Graphics
S2 ITS : Image Watermarking and Steganography
S3 UGM : Digital Evidence Cabinets

- Koordinator Konsentrasi Forensika Digital, Magister Informatika FTI UII Yogyakarta
- Staff Pengajar S1 Informatika FTI UII
- Kepala Pusat Studi Forensika Digital (PUSFID) UII Yogyakarta
- Ketua Bidang Sertifikasi, Standarisasi dan Akreditasi, AFDI (Asosiasi Forensik Digital Indonesia)
- Chairman of HADFEX (Hacking and Digital Forensics Exposed)

- CHFI , Encase, Oxygen, Belkasoft, EnScript
- Hacker In The Box (2012), Hacker Halted (2012)

FORENSIKA DIGITAL
UNIVERSITAS ISLAM INDONESIA

h@dfex
hacking and digital forensics exposed

PUSAT STUDI FORENSIKA DIGITAL
PUSFID
UNIVERSITAS ISLAM INDONESIA

Agenda

- Digital Lifestyle
- Cybercrime
- Cyberlaw dan UU
- Forensik Digital
- Bukti Digital
- Metodologi Forensik

Digital Native vs Digital Immigrants

Digital Immigrants

- Adopters of the web technologies
- Prefer to talk in person
- Logical learners
- Focusing on one task at a time
- Prefer to have interaction with one or few people rather than many
- Get info from traditional news sites

Digital Natives

- Born during or after the digital age
- Always on, attached to a phone or other device
- Intuitive learners
- Multitask and rapidly task-switch
- Extremely social
- Multimedia oriented

Digital Lifestyle

JAN 2020

OVERVIEW OF INTERNET USE

NUMBER OF PEOPLE USING THE INTERNET, AND HOW MUCH TIME THEY SPEND USING THE INTERNET EACH DAY

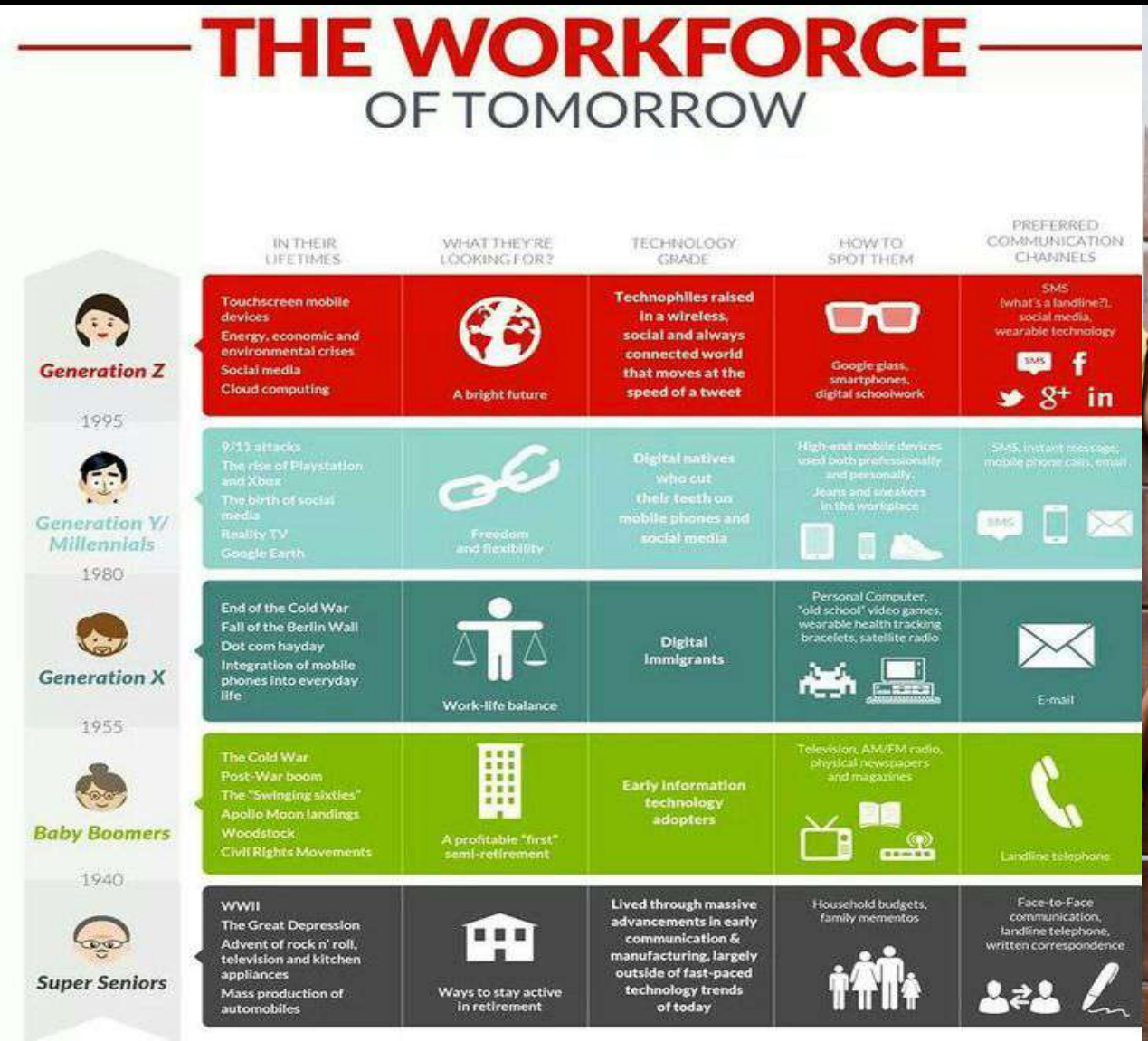
INDONESIA

https://datareportal.com/digital-in-indonesia

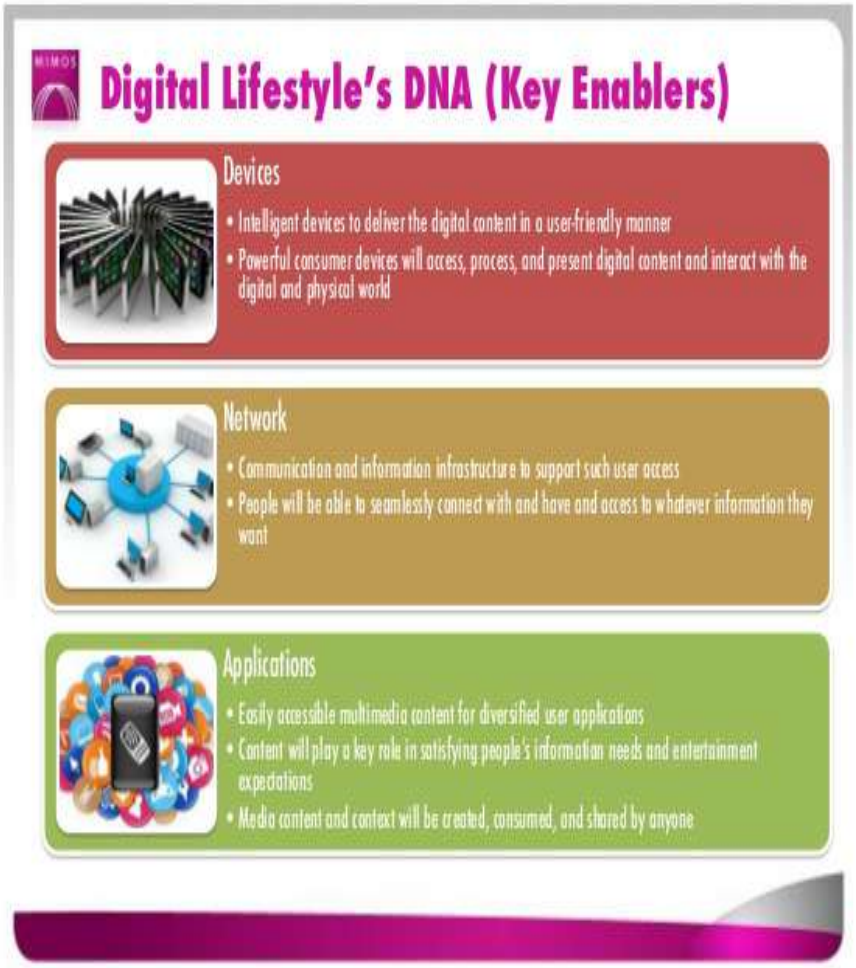
SOURCES: ITU; GLOBALWEBINDEX; GSMA INTELLIGENCE; EUROSTAT; SOCIAL MEDIA PLATFORMS' SELF-SERVICE ADVERTISING TOOLS; LOCAL GOVERNMENT BODIES AND REGULATORY AUTHORITIES; APJII; UNITED NATIONS (ALL LATEST AVAILABLE DATA IN JANUARY 2020). TIME SPENT DATA FROM GLOBALWEBINDEX (Q3 2019), BASED ON A BROAD SURVEY OF INTERNET USERS AGED 16 TO 64. SEE GLOBALWEBINDEX.COM FOR MORE DETAILS. ◆ COMPARABILITY ADVISORY: SOURCE CHANGES.

we are social Hootsuite

Gaya Komunikasi



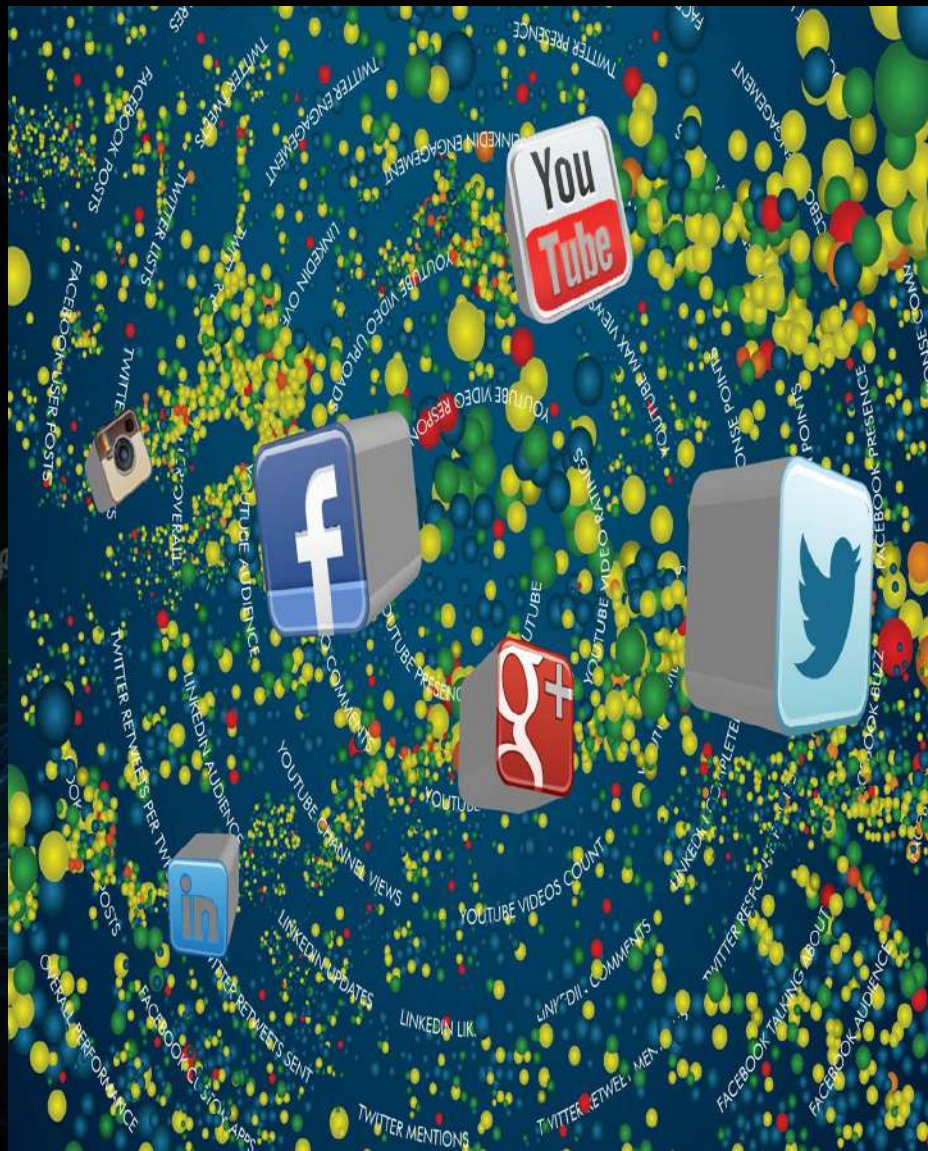
Digital Lifestyle



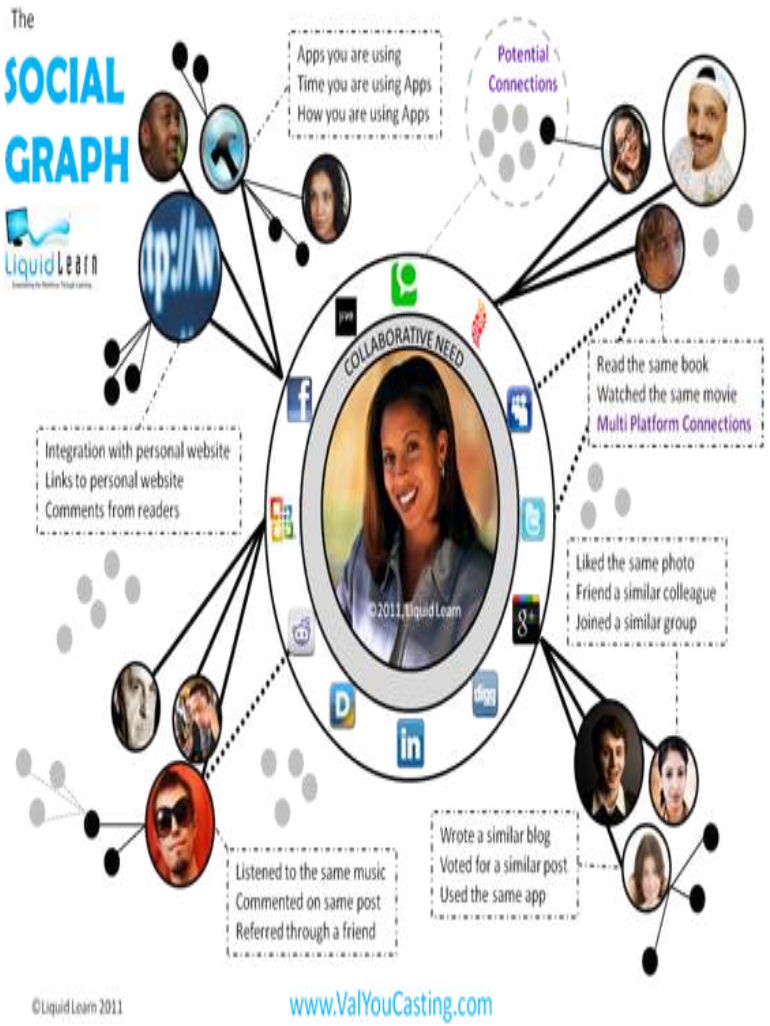
Cyberspace

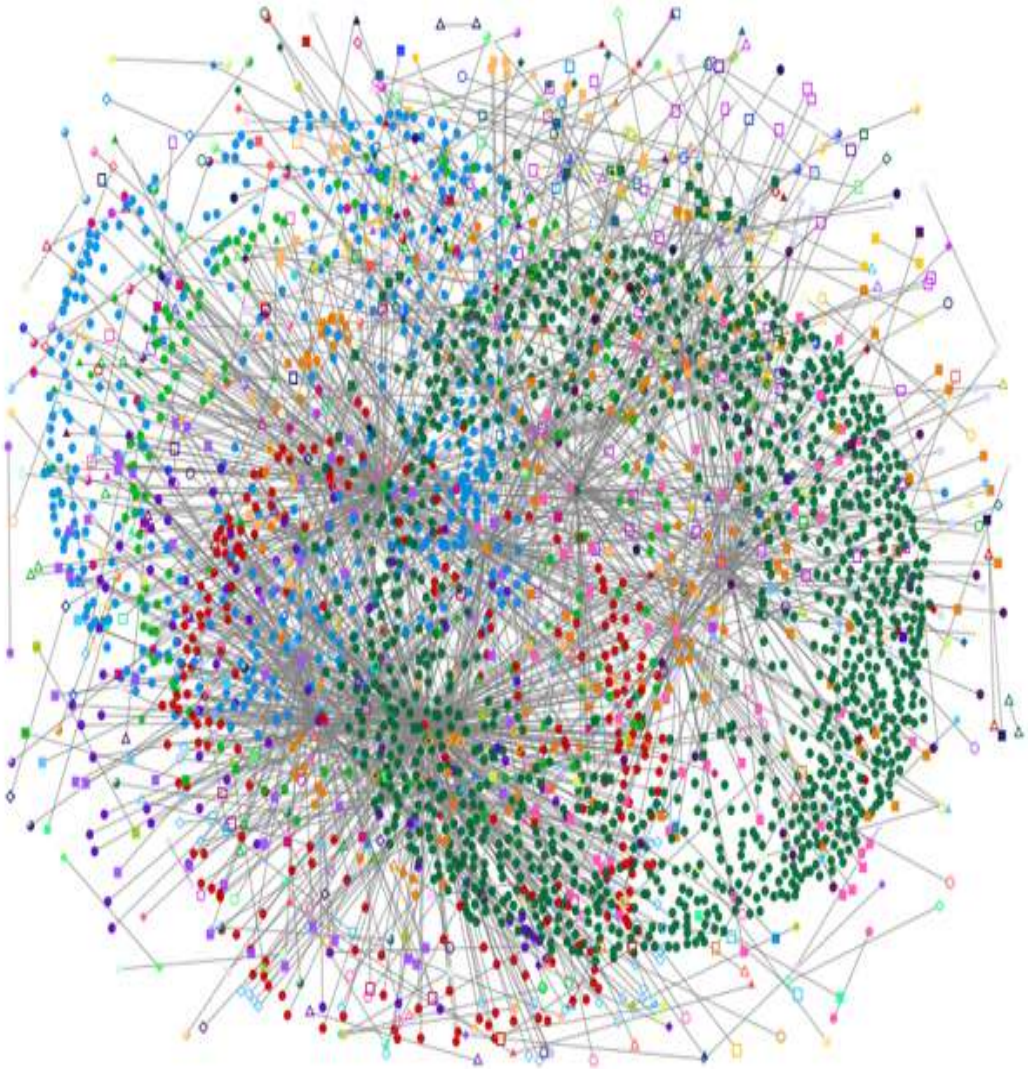
- Cyberspace is first and foremost an information environment. It is made up of digitized data that is created, stored, and, most importantly, shared.
- Today Cyberspace is a household name and has been recognised as the **fifth domain of warfare.**

Digital Universe



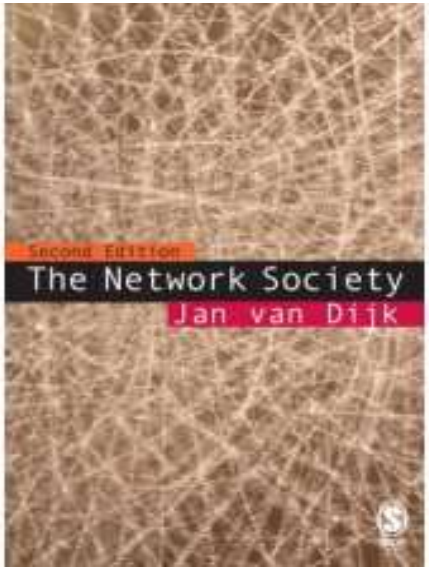
The Power of Social Graph

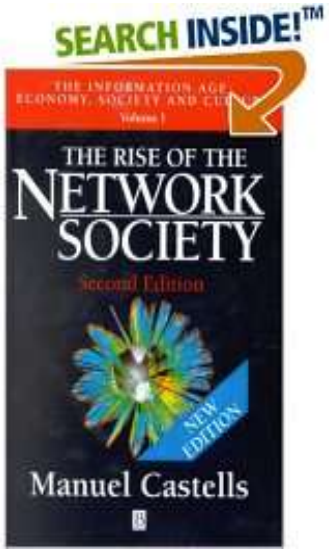


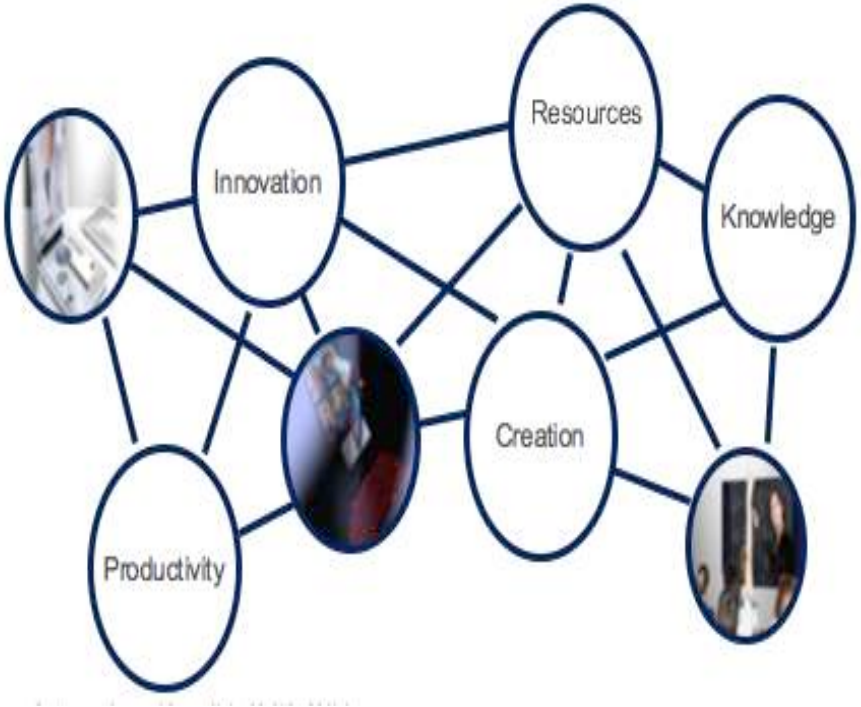


Networked Society

A new techno-economic system (society) where the key social structures and activities are organized around electronically processes information networks





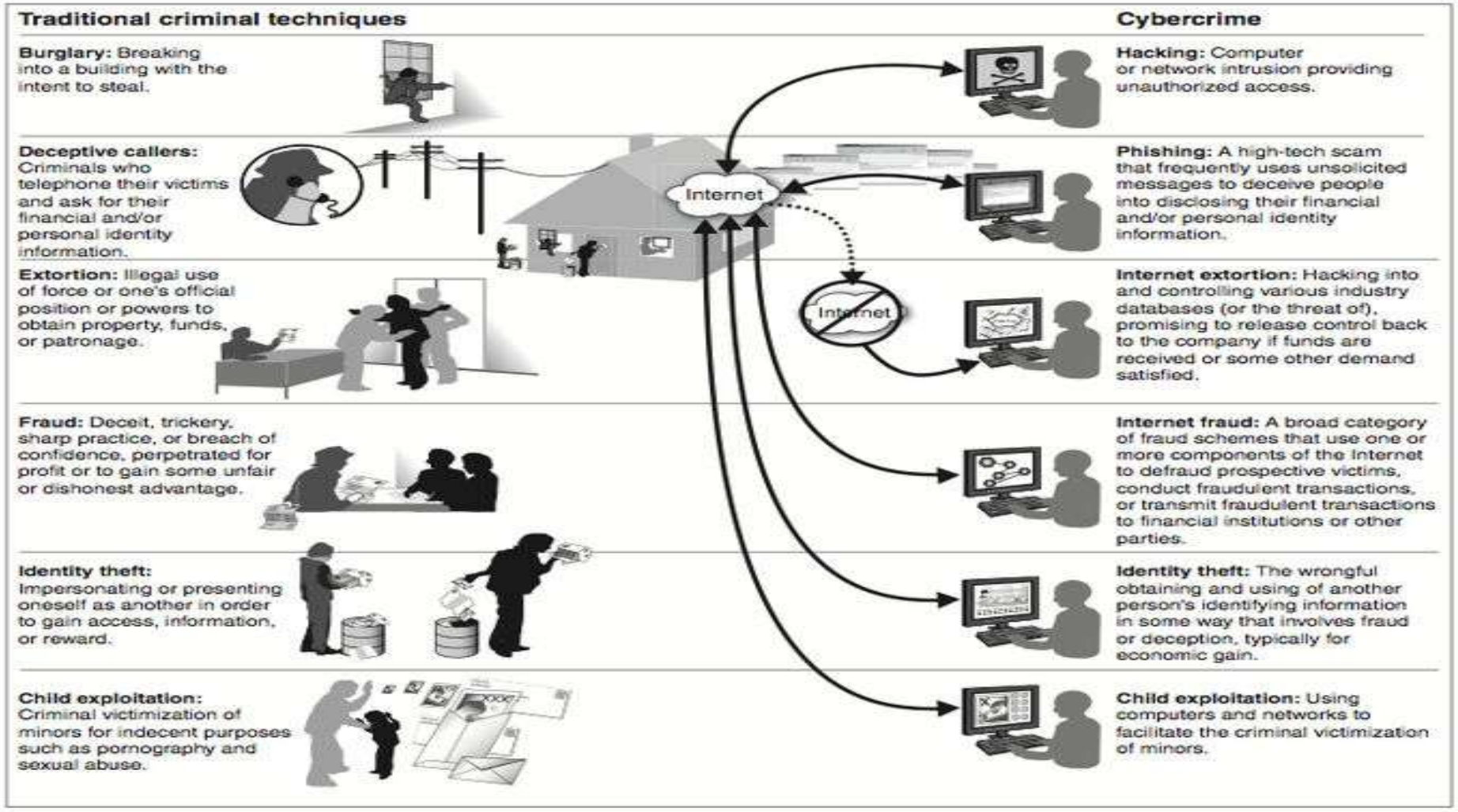


In the networked society people, knowledge, devices, and information are networked for the growth of society, life and business.

Traditional vs Cyber (crime)

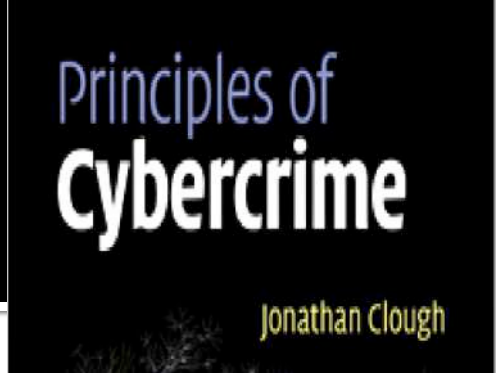
http://itlaw.wikia.com/wiki/Cybercrime

Figure 1: Comparison between Traditional Criminal Techniques and Cybercrime



Source: GAO

Klasifikasi Cybercrime



- Crimes in which the computer or computer network is the target of the criminal activity. For example, hacking, malware and DoS attacks.
- Existing offences where the computer is a tool used to commit the crime. For example, child pornography, stalking, criminal copyright infringement and fraud.
- Crimes in which the use of the computer is an incidental aspect of the commission of the crime but may afford evidence of the crime. For example, addresses found in the computer of a murdesuspect, or phone records of conversations between offender and victim before a homicide. In such cases the computer is not significantly implicated in the commission of the offence, but ismore a repository for evidence

- computer crimes,
- Computer facilitated crimes
- computer-supported crimes

Cyberlaw dan UU ITE

- UU NKRI Terkait :
  - UU KUHP
  - UU 11 / 2008 : ITE
  - UU 44/2008 : Pornografi
  - UU 19/2002 : Hak Cipta
  - UU 15/2003 : Terorisme
  - UU 25/2003 : Pencucian Uang
  - UU 5/ 1999 : Persaingan Usaha
  - UU 20/2001 : Tipikor

UU 20 2001

- Pasal 26 A
  - Alat bukti yang sah dalam bentuk petunjuk sebagaimana dimaksud dalam Pasal 188 ayat (2) Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana, khusus untuk tindak pidana korupsi juga dapat diperoleh dari :
    a. alat bukti lain yang berupa informasi yang diucapkan, dikirim, diterima, atau disimpan secara elektronik dengan alat optik atau yang serupa dengan itu; dan
    b. dokumen, yakni setiap rekaman data atau informasi yang dapat dilihat, dibaca, dan atau didengar yang dapat dikeluarkan dengan atau tanpa bantuan suatu sarana, baik yang tertuang di atas kertas, benda fisik apapun selain kertas, maupun yang terekam secara elektronik, yang berupa tulisan, suara, gambar, peta, rancangan, foto, huruf, tanda, angka, atau perforasi yang memiliki makna.

Perbuatan yang dilarang

- Perbuatan:
  - Menjanjikan sesuatu
  - Menerima hadiah
  - Gratifikasi
  - Dll
- Perbuatan yang dilarang yang dilakukan yang difasilitasi oleh adanya TI.
  - Dokumen (audio, video, image, text)
  - History, fakta dan data perbuatan

Pasal UU yang dilanggar	Pasal 35 : Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.
	Kasus: • Si A memiliki dokumen NIK/KK yang didapat dari situs dark web. • Si A dan Si B melakukan komunikasi via WA kemudian memberikan dokumen NIK/KK yang dimilikinya kepada si B melalui kiriman dokumen WA. • Si B menggunakan data yang ada pada dokumen NIK/KK untuk melakukan registrasi kartu SIM CARD Prabayar yang dijual di sebuah outlet • Si B Menjual Kartu SIM CARD ready yg telah teregistrasi. • SI A mendapat komisi dari setiap penjualan kartu SIMCARD oleh si B. Si A dan Si B kemudian ditangkap untuk dimintai pertanggungjawabannya terhadap penggunaan NIK/KK yang tidak syah untuk registrasi. Kepada keduanya dikenakan Pasal 35 UU ITE. Barang bukti yang diamankan adalah HP X milik si A dan HP Y milik si B. Bukti apa saja yang harus disiapkan agar pidana Pasal 35 UU ITE dpt diterapkan pada keduanya.

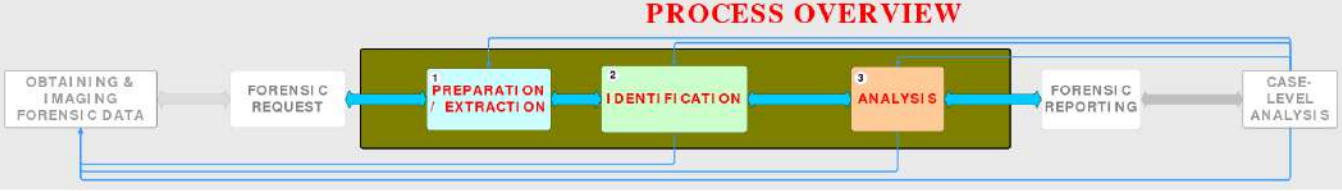
Aspek	Unsur	Analisa Kasus dan Bukti	
		Perbuatan	Bukti yg harus didapat/dicari ?
Kesalahan	dengan sengaja	dengan sengaja menggunakan dokumen untuk registrasi	keberadaan dokumen serta history transaksi registrasi dengan dokumen tsb.
Melawan hukum	tanpa hak	tanpa hak memiliki dan menggunakan dokumen	Keberadaan file dokumen pada device milik tersangka
Perbuatan	manipulasi, penciptaan, perubahan, penghilangan, pengrusakan	manipulasi registrasi dengan memasukkan Nama, NIK, KK tanpa hak	History registrasi dengan data yang termuat pada dokumen yang dimiliki tersangka
Objek	informasi elektronik dan/atau dokumen elektronik	informasi elektronik dan/atau dokumen elektronik, berupa data KK dan NIK	Dokumen yang berisi NIK dan KK
Tujuan	agar informasi dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik	agar informasi dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik, untuk kepentingan registrasi Sim Card	History registrasi yang sukses serta efek lain dari keberhasilan registrasi yang didapat oleh tersangka.

Forensika Digital

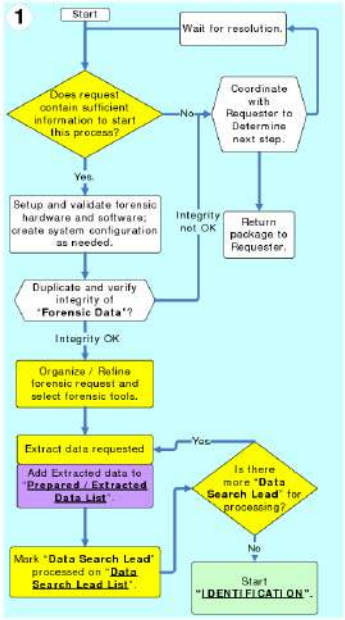
DIGITAL FORENSIC ANALYSIS METHODOLOGY

Last Updated: August 20, 2007

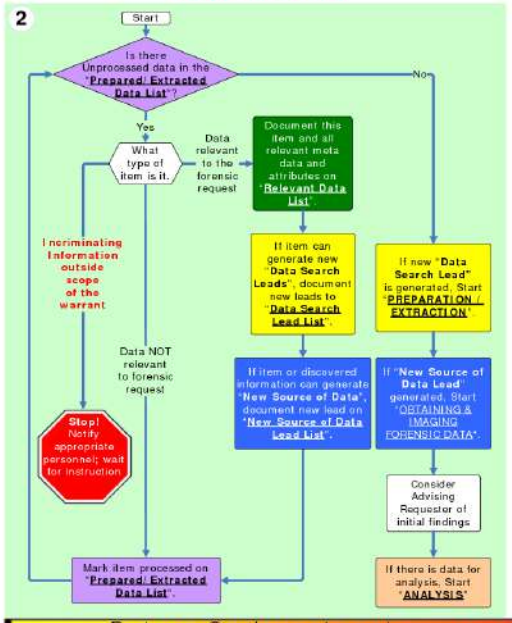
PROCESS OVERVIEW



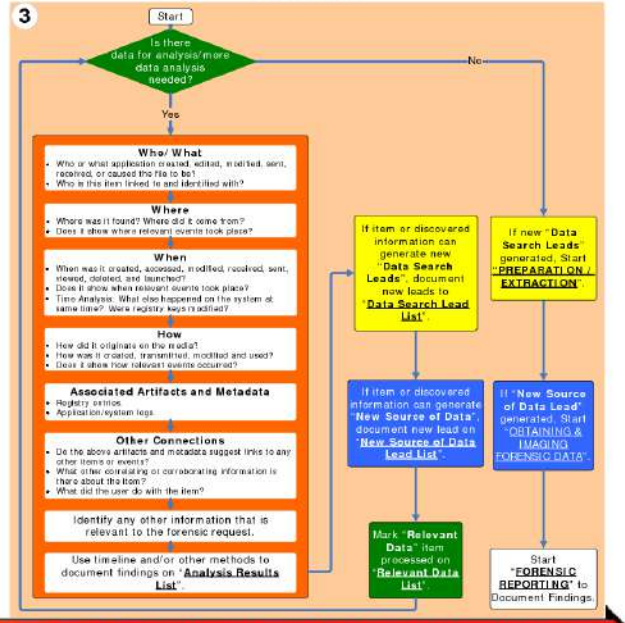
PREPARATION / EXTRACTION



IDENTIFICATION

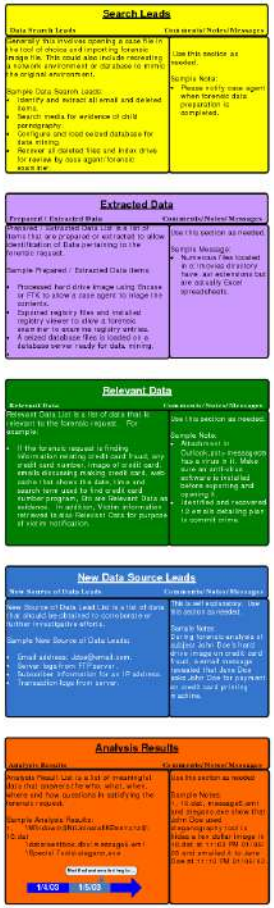


ANALYSIS



Return On Investment (Determine when to stop this process. Typically, after enough evidence is obtained for prosecution, the value of additional forensic analysis diminishes.)

LISTS



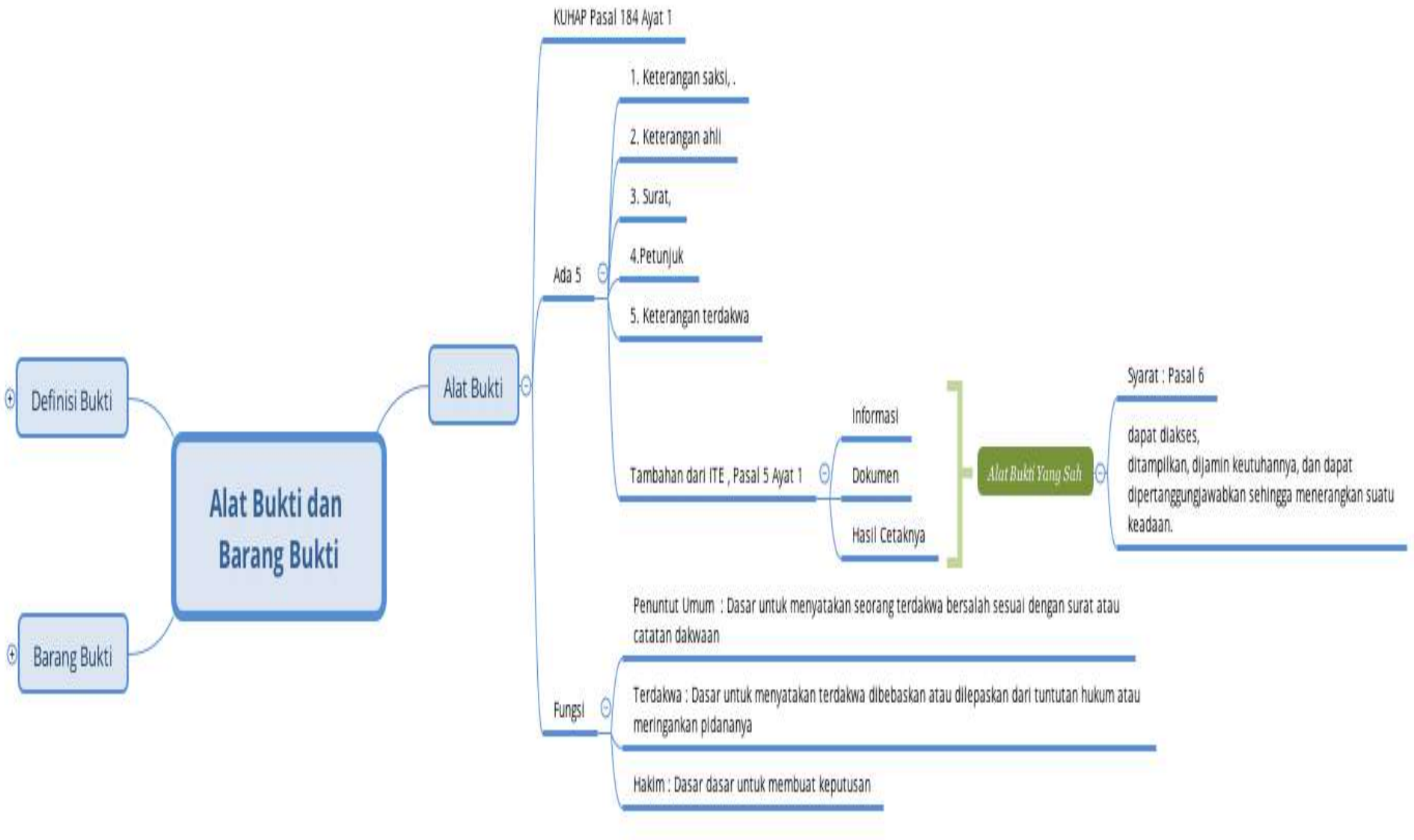
Terminologi

- "Digital forensics" was originally simply data recovery.
  - “retrieving information that was deleted by mistake or lost during a power surge or server crash”
  - Digital forensics developed as an independent field in the late 1990s and early 2000s when computer based crime started growing with the increasing usage of computers and more so, the Internet.

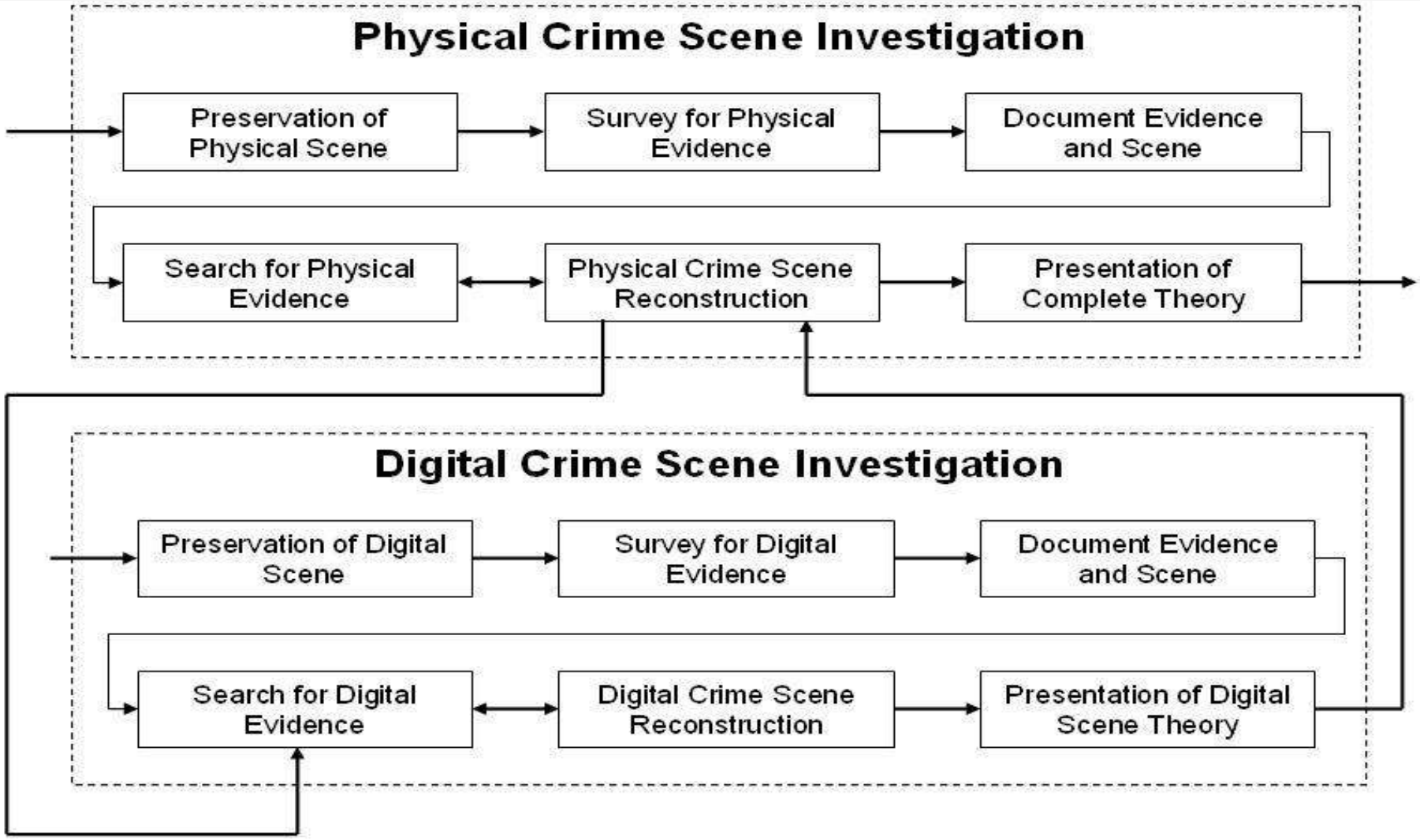
- Forensics → Scientific Methods.
  - *“Digital Forensics is a branch of computer science that focuses on developing evidence pertaining to digital files for use in civil or criminal court proceedings”*

Barang Bukti

Alat Bukti

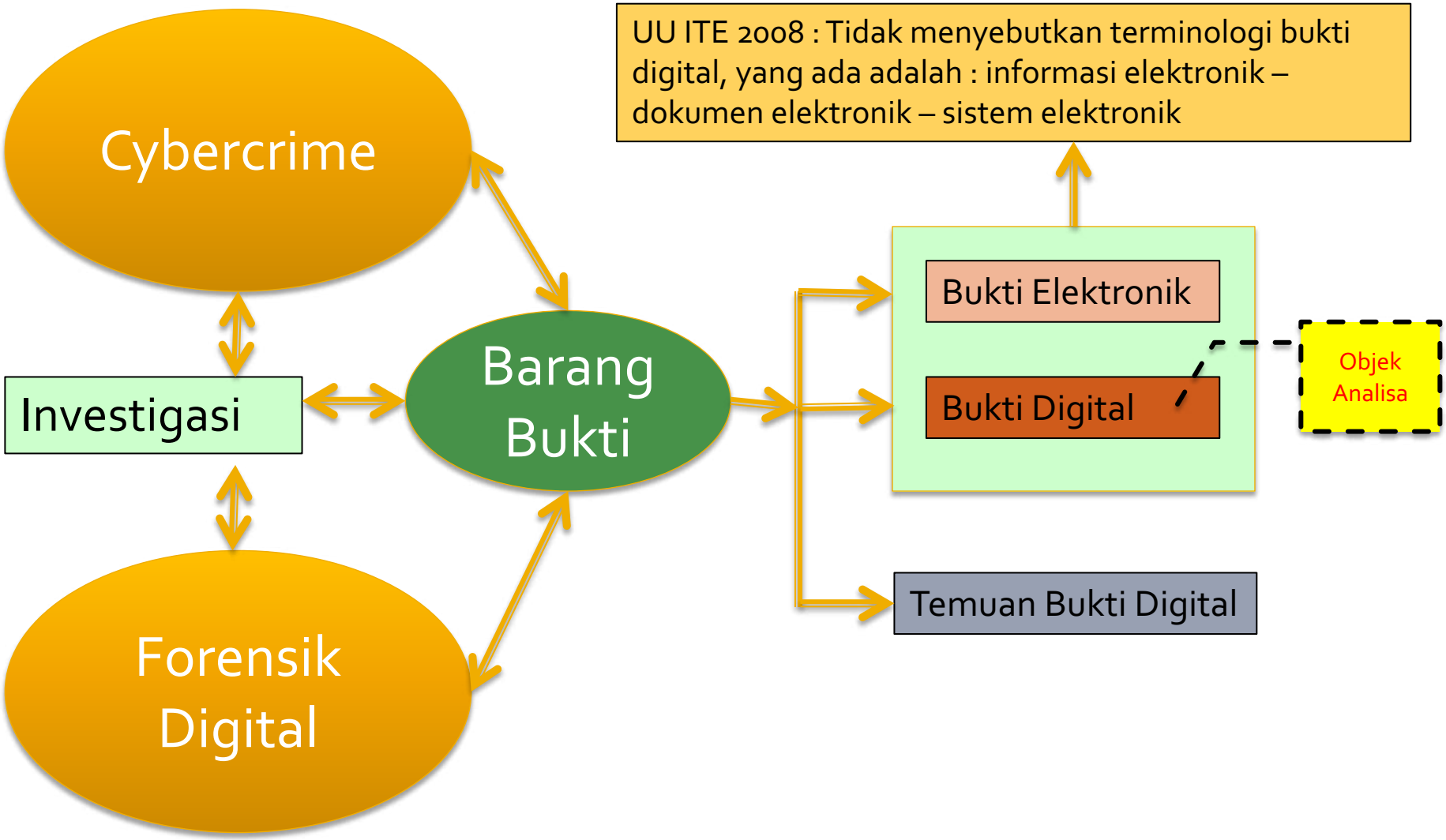

Alat Bukti dan Barang Bukti
Definisi Bukti
Barang Bukti
Alat Bukti
KUHAP Pasal 184 Ayat 1
Ada 5
1. Keterangan saksi, .
2. Keterangan ahli
3. Surat,
4.Petunjuk
5. Keterangan terdakwa
Tambahan dari ITE , Pasal 5 Ayat 1
Informasi
Dokumen
Hasil Cetaknya
Alat Bukti Yang Sah
Syarat : Pasal 6
dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan.
Fungsi
Penuntut Umum : Dasar untuk menyatakan seorang terdakwa bersalah sesuai dengan surat atau catatan dakwaan
Terdakwa : Dasar untuk menyatakan terdakwa dibebaskan atau dilepaskan dari tuntutan hukum atau meringankan pidananya
Hakim : Dasar dasar untuk membuat keputusan

Physical + Digital Investigation



Bukti Digital

Terminologi



Bukti Digital

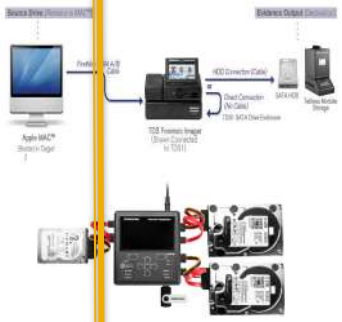
Terminologi

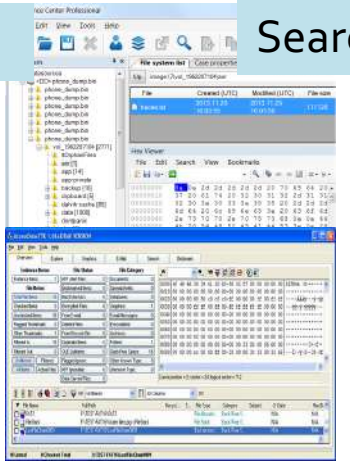
Bukti Elektronik	Bukti Digital	Temuan Bukti Digital
Multimedia File	Audio, Image, Video,	Analisa Orisinalitas, Fakta

Offline

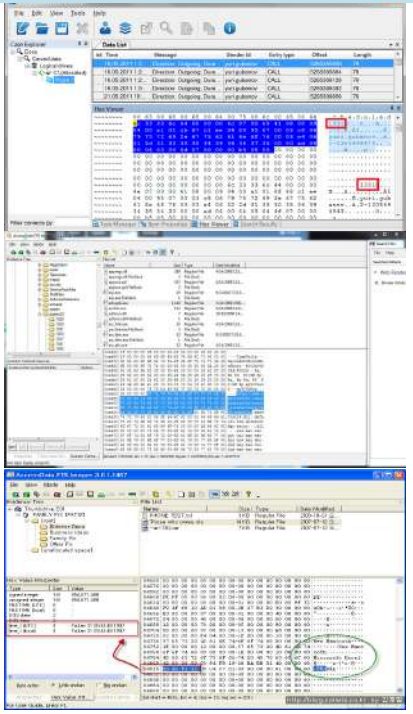
Online

Akuisisi dan Imaging

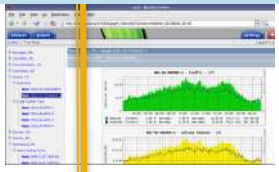


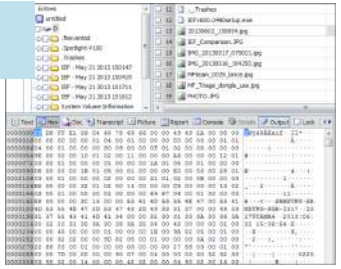


Searching - Eksplorasi dan Analisa



Capture, record, log





Digital Evidence

Characteristics of Digital Evidence

The digital evidence must have some characteristics to be disclosed in the court of law

Admissible

Evidence must be related to the fact being proved

Believable

Evidence must be clear and understandable by the judges

Authentic

Evidence must be real and related to the incident in a proper way

Reliable

There must be no doubt about the authenticity or veracity of the evidence

Complete

Evidence must prove the attacker's actions or his innocence

Function of Digital Evidence

- Prove or disprove criminal activity
- Prove or disprove policy violation
- Prove or disprove malicious behavior to or by the computer/user

If the evidence is there, the case is yours to lose with very little effort.

Forensics and Court

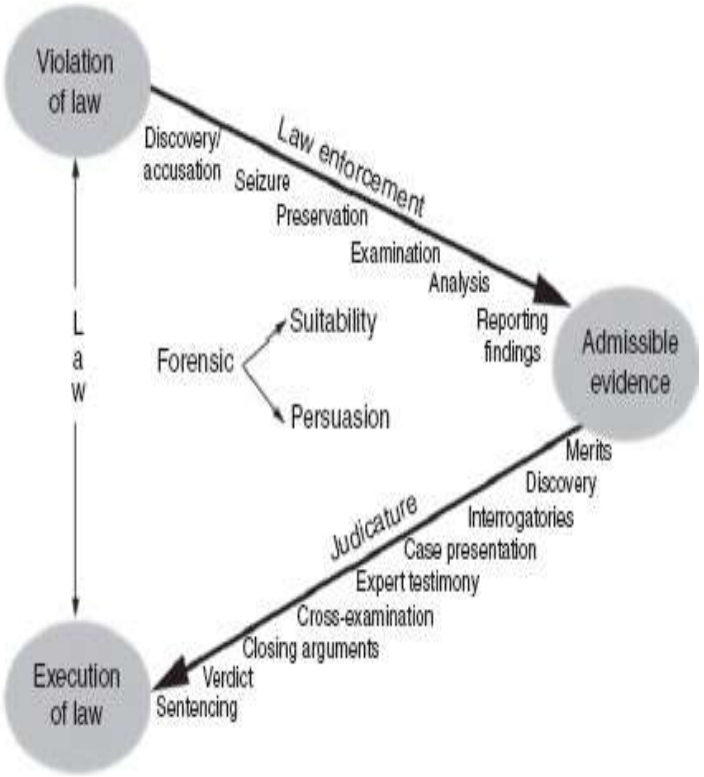
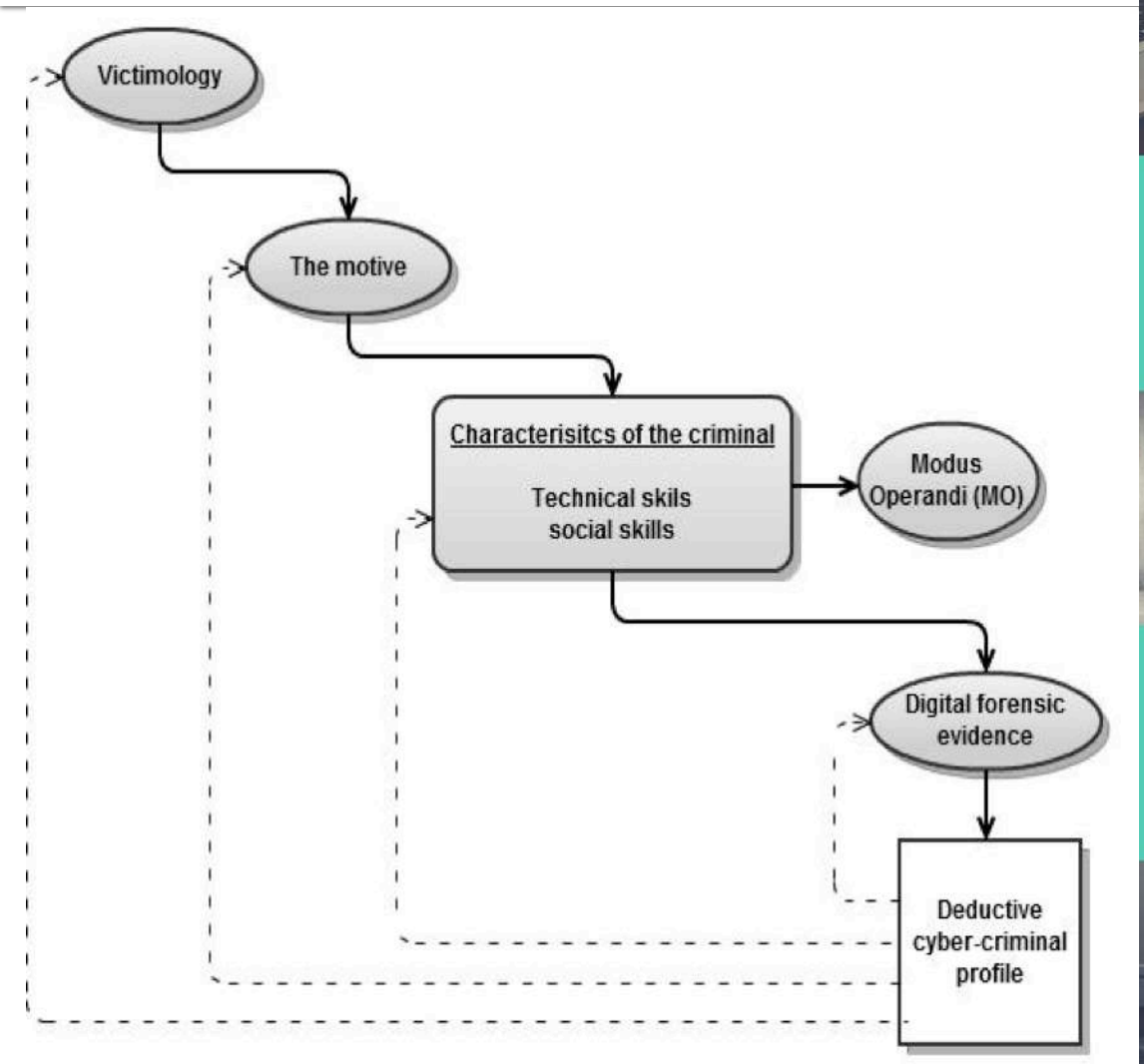


FIGURE 3.1
Overview of case/incident resolution process.

Profiling


Victimology
The motive
Characterisitcs of the criminal
Technical skils
social skills
Modus Operandi (MO)
Digital forensic evidence
Deductive cyber-criminal profile


HOW TO CRIME ANALISYS
FOR
Digital Forensic
www.ilmuforensikadigital.blogspot.com | ahmad.subki1992@gmail.com
1
the scenarios
menarasikan ulang kejadian secara berurut, sehingga dapat menggambarkan bagaimana peristiwa tersebut terjadi
the law
petakkan aspek hukum dan aturan apa saja yang dilanggar ketika melakukan kejahatan tersebut.
2
3
who is liable?
siapa saja yang terlibat dalam kasus kejahatan tersebut dan apa perannya
motive & modus
deskripsikan tujuan pelaku melakukan kejahatan tersebut dan jelaskan apa saja langkah-langkah yang dilakukan untuk melancarkan kejahatannya
4
HACKER
SPY
VIRUS
THIEF
5
digital evidence
jelaskan apa saja barang bukti digital maupun elektronik yang ditemukan dan dimana tempat ditemukannya

Metodologi

Stage 1 Investigation preparation	a. identify the purpose of investigation
	b. identify resources required
Stage 2 Evidence acquisition	a. identify sources of digital evidence
	b. preserve digital evidence
Stage 3 Analysis of evidence	a. identify tools and techniques to use
	b. process data
	c. interpret analysis results
Stage 4 Results dissemination	a. report findings
	b. present findings

Aktivitas Forensik Digital

Crime Scene Investigation

Akuisisi dan Imaging

Dokumentasi dan Presentasi

Eksplorasi dan Analisis

Digital Forensics

Potential Evidence Source

Digital storage devices

File Types Extracted

All data collected and copied using extraction tools

File Clusters

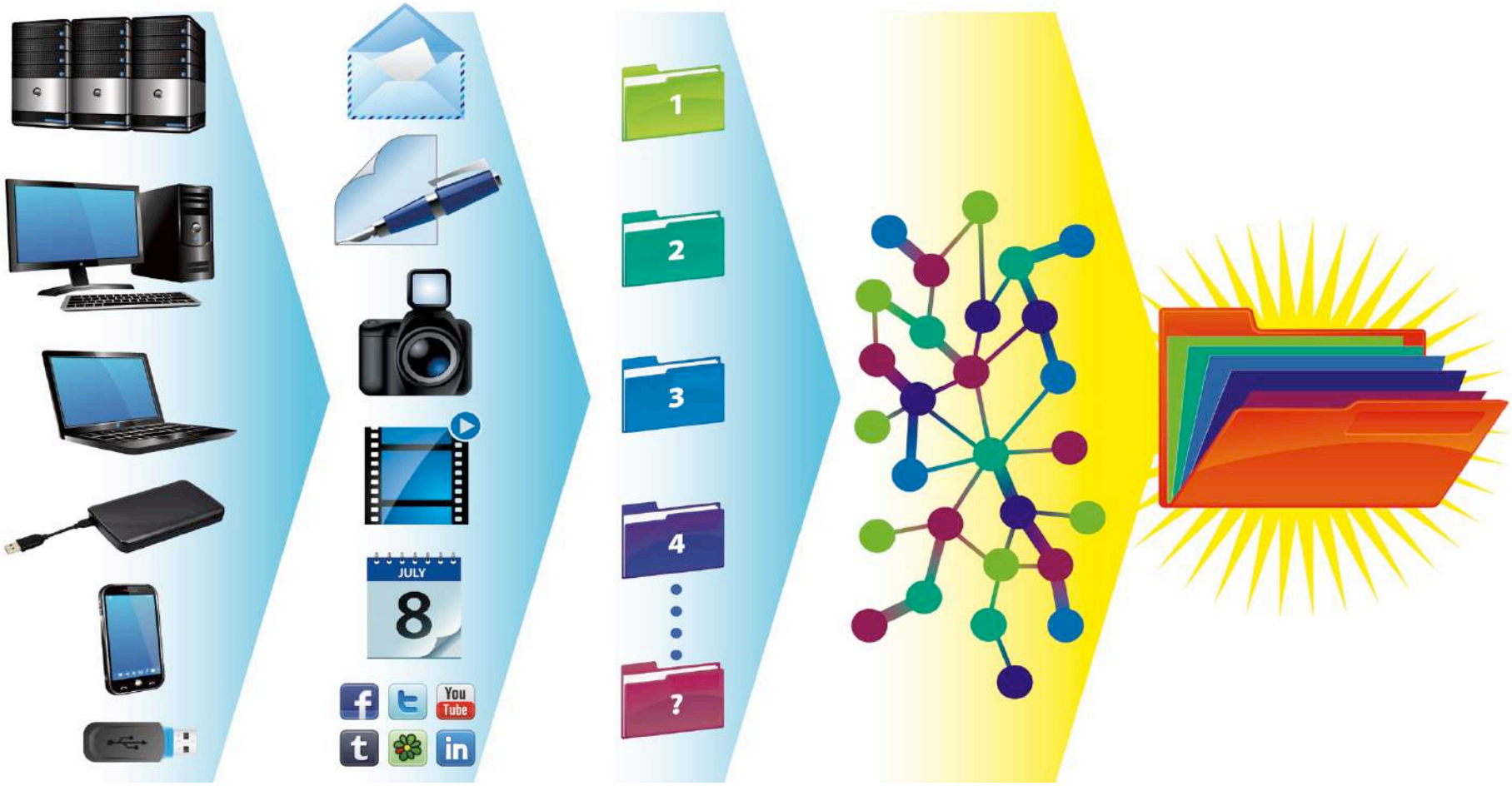
Files matched by similarity and association. Indexing, search enabled. All metadata retained.

Connections Discovered

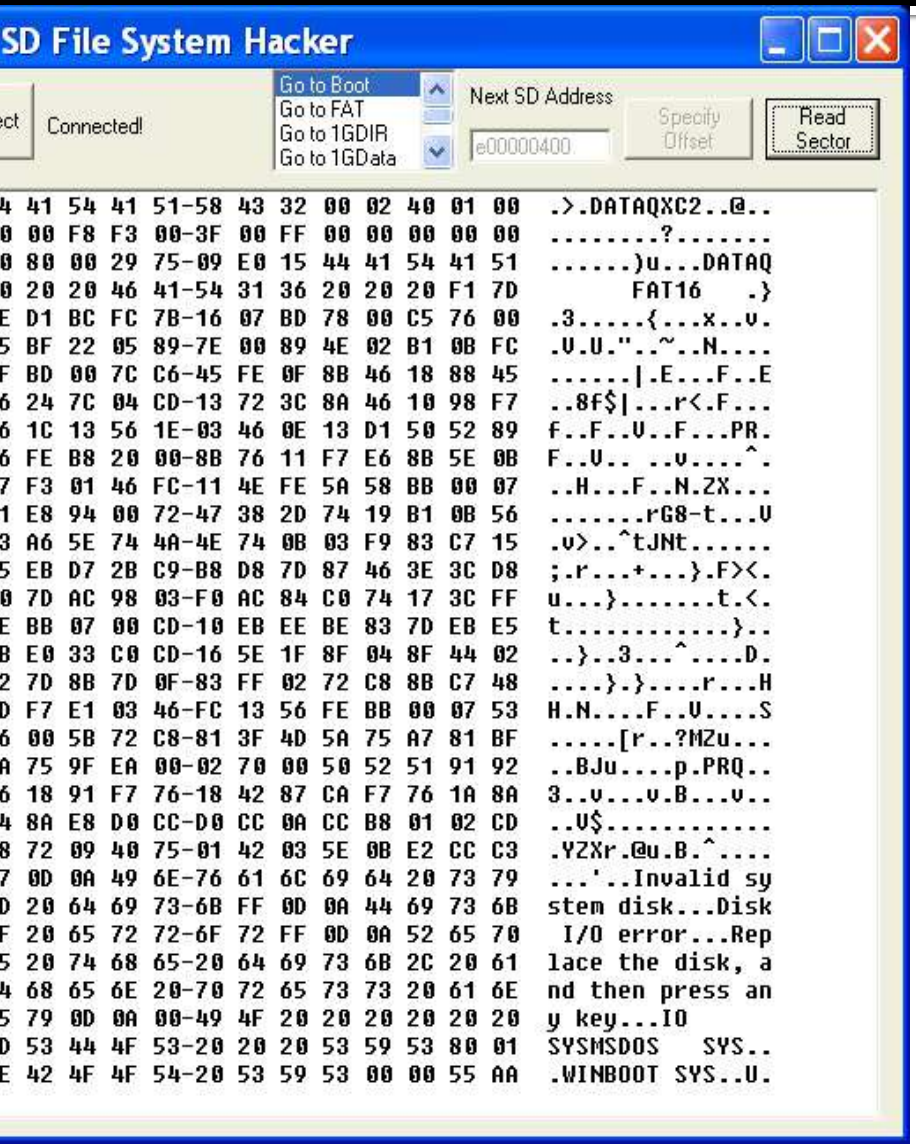
By off-the-shelf servers running Bolero™

Suspect/Possibly Incriminating Files

Ready for detailed examination - ***FAST***



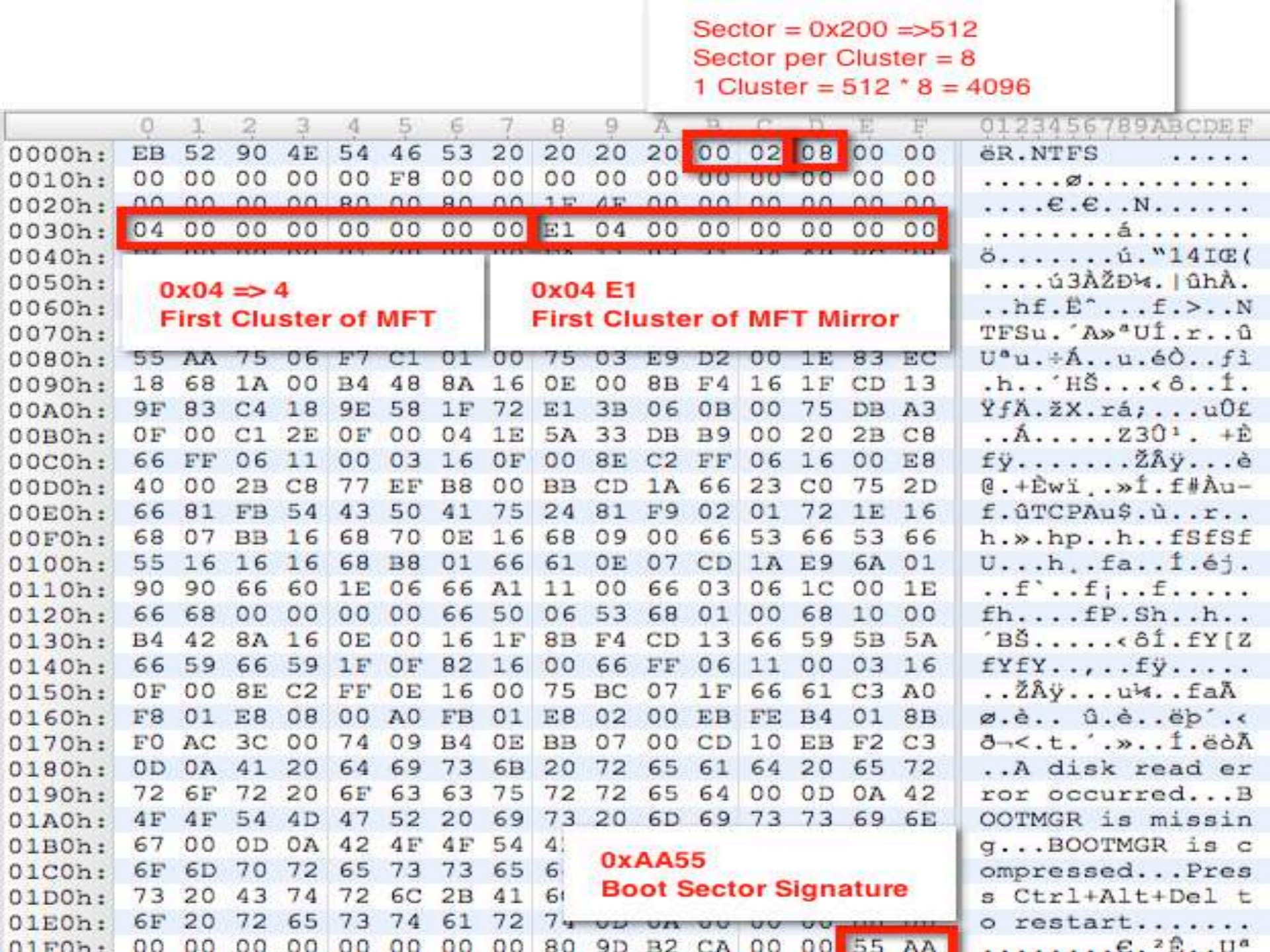
The Art of Digital Forensics



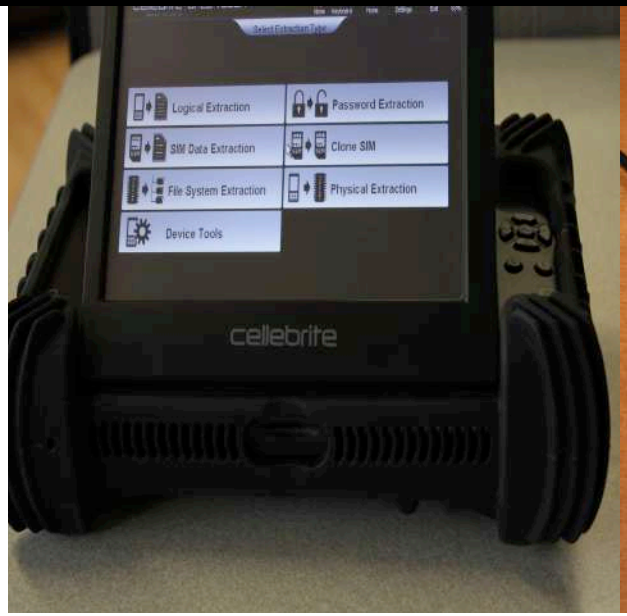
Objek Utama :
Bukti Elektronik dan Bukti Digital

Aktivitas Utama : Searching

Pertanyaan Utama :
What – Where – When – Who – Why and How


Sector = 0x200 =>512
Sector per Cluster = 8
1 Cluster = 512 * 8 = 4096
0x04 => 4
First Cluster of MFT
0x04 E1
First Cluster of MFT Mirror
0xAA55
Boot Sector Signature

Hardware dan Software



nuix
CRU
Digital Intelligence
EnCase
X-Ways
AccessData
VOOM Technologies, Inc.
MD5
SALVATIONDATA TECHNOLOGY www.recoverytoolsrus.com
Atola TECHNOLOGY
Belkasoft Forensics made easier
DEEPSPAR Data Recovery Systems
Passware
TABLEAU Solutions for the Digital Evidence Lifecycle
OXYGEN SOFTWARE
ADF SOLUTIONS, INC.
SEH
GetData Software Development Company
MAGNET FORENSICS
Logicube
Guidance SOFTWARE
SC
My Hard Drive Died
Intella
BlackBag TECHNOLOGIES
SiQuest

Kesiapan APH

Forensik Digital di BPKP

www.bpkp.go.id/investigasi/konten/2207/Pedoman-Pengumpulan-dan-Pengevaluasian-Bukt

Beranda | Berita | Tentang Kami | Unit Kerja | Peraturan | Informasi

BADAN PENGAWASAN KEUANGAN DAN PEMBANGUNAN
Kawal Akuntabilitas Keuangan dan Pembangunan

Deputi Bidang Investigasi

Pedoman Pengumpulan dan Pengevaluasian Bukti Dokumen Elektronik

Perkembangan teknologi informasi selain mempermudah kehidupan manusia juga memunculkan risiko computer crime(akses secara ilegal ke dalam suatu sistem, pencurian data penting dari target tertentu, dll) serta computer-related crime (pencurian, pornografi, narkoba, dan korupsi, dll dengan menggunakan komputer sebagai alat merencanakan, melaksanakan, dan menyimpan hasil kejahatan).

Perkembangan tersebut direspon dengan terbitnya UU Nomor 11/2008 tentang Informasi dan Transaksi Elektronik yang menyatakan bahwa informasi dan/atau data elektronik merupakan alat bukti hukum yang sah dan bisa digunakan dalam hukum acara yang berlaku di Indonesia

Dalam rangka meningkatkan kerjasama dengan aparat penegak hukum dan meningkatkan pelayanan, Deputi Bidang Investigasi membangun Laboratorium Komputer Forensik yang membantu Aparat Penegak Hukum untuk mendapatkan Bukti Dokumen Elektronik yang tata cara pelaksanaannya diatur dalam Peraturan Tersendiri.

Laboratorium Komputer Forensik sendiri telah berkali-kali berhasil membantu mengungkap kasus tindak pidana korupsi bersama-sama dengan penyidik dengan menyediakan bukti analisa terhadap barang bukti elektronik.

Diskusi

TERIMA KASIH