



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)



hadfex
hacking and digital forensics exposed

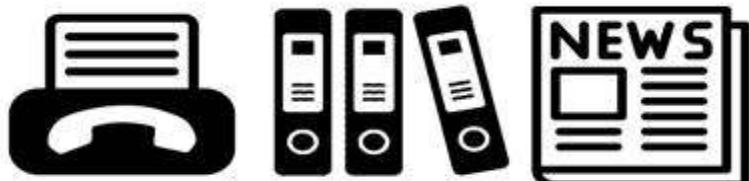


Agenda

- 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

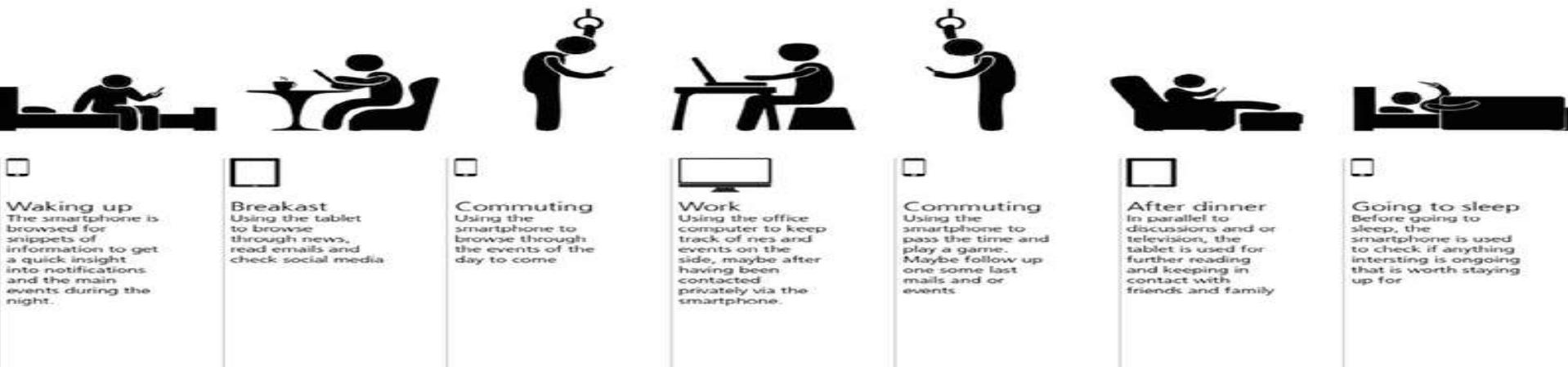
Digital Natives



- 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

OUR DIGITAL DAY



JAN
2020

OVERVIEW OF INTERNET USE

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



TOTAL NUMBER
OF INTERNET USERS
ON ANY DEVICE



175.4
MILLION

INTERNET USERS
AS A PERCENTAGE OF
TOTAL POPULATION



64%

ANNUAL GROWTH
IN THE NUMBER
OF INTERNET USERS



+17%
+25 MILLION

AVERAGE DAILY TIME SPENT
USING THE INTERNET ON ANY
DEVICE BY EACH INTERNET USER



7H 59M

SOURCES: ITU; GLOBALWEBINDEX; GSMA INTELLIGENCE; EUROSTAT; SOCIAL MEDIA PLATFORMS' SELF-SERVICE ADVERTISING TOOLS; LOCAL GOVERNMENT BODIES AND REGULATORY AUTHORITIES; APJI; 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](https://globalwebindex.com) FOR MORE DETAILS. ♦ COMPARABILITY ADVISORY: SOURCE CHANGES.

Gaya Komunikasi

— THE WORKFORCE — OF TOMORROW

	IN THEIR LIFETIMES	WHAT THEY'RE LOOKING FOR	TECHNOLOGY GRADE	HOW TO SPOT THEM	PREFERRED COMMUNICATION CHANNELS
Generation Z 1995	Touchscreen mobile devices Energy, economic and environmental crises Social media Cloud computing	A bright future	Technophiles raised in a wireless, social and always connected world that moves at the speed of a tweet	Google glass, smartphones, digital schoolwork	SMS (what's a landline?), social media, wearable technology     
Generation Y/ Millennials 1980	9/11 attacks The rise of Playstation and Xbox The birth of social media Reality TV Google Earth	Freedom and flexibility	Digital natives who cut their teeth on mobile phones and social media	High-end mobile devices used both professionally and personally. Jeans and sneakers in the workplace	SMS, instant messaging, mobile phone calls, email   
Generation X 1955	End of the Cold War Fall of the Berlin Wall Dot com hayday Integration of mobile phones into everyday life	Work-life balance	Digital Immigrants	Personal Computer, "old school" video games, wearable health tracking bracelets, satellite radio	
Baby Boomers 1940	The Cold War Post-War boom The "Swinging sixties" Apollo Moon landings Woodstock Civil Rights Movements	A profitable "first" semi-retirement	Early information technology adopters	Television, AM/FM radio, physical newspapers and magazines	
Super Seniors	WWII The Great Depression Advent of rock n' roll, television and kitchen appliances Mass production of automobiles	Ways to stay active in retirement	Lived through massive advancements in early communication & manufacturing, largely outside of fast-paced technology trends of today	Household budgets, family mementos	Face-to-Face communication, landline telephone, written correspondence   



Digital Lifestyle



Digital Lifestyle's DNA (Key Enablers)



Devices

- Intelligent devices to deliver the digital content in a user-friendly manner
- Powerful consumer devices will access, process, and present digital content and interact with the digital and physical world



Network

- Communication and information infrastructure to support such user access
- People will be able to seamlessly connect with and have and access to whatever information they want



Applications

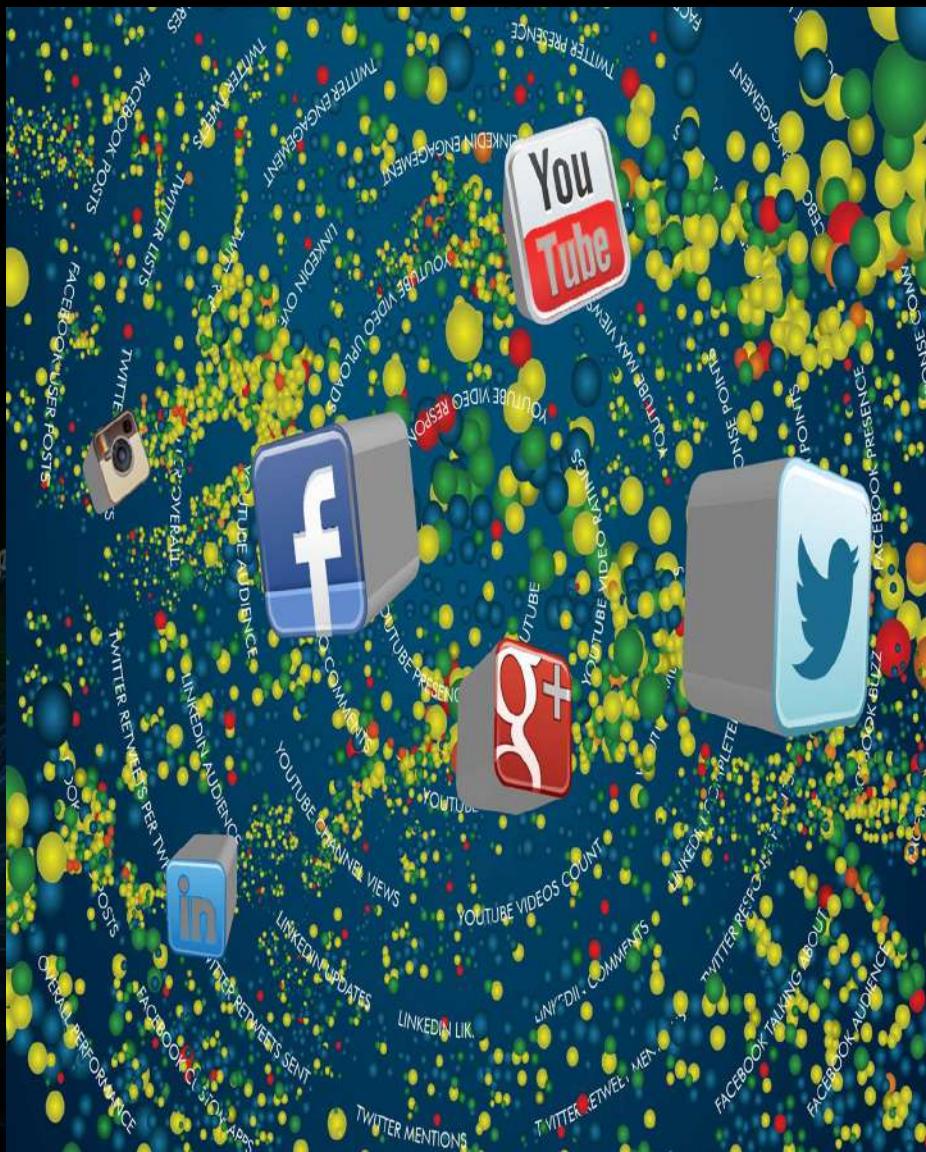
- Easily accessible multimedia content for diversified user applications
- Content will play a key role in satisfying people's information needs and entertainment expectations
- Media content and context will be created, consumed, and shared by anyone

Cyberspace

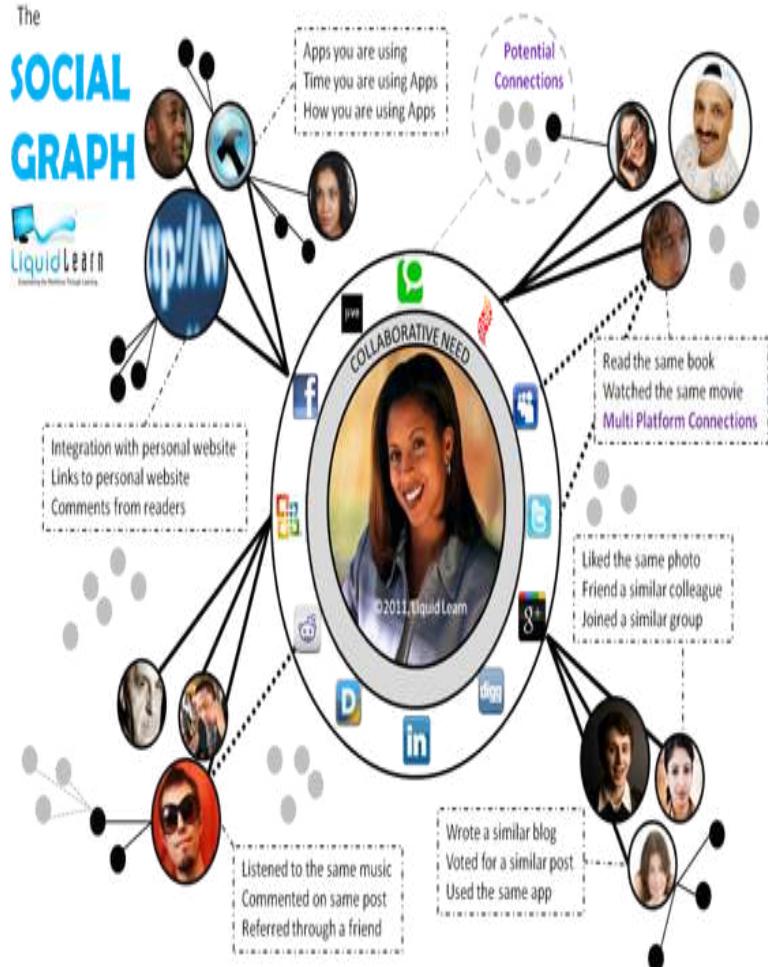


- Cyberspace is first and foremost an information environment. It is made up of **digitized data that is created, stored, and, most importantly, shared.**
- Today Cyberspace is a household name and has been recognised as the **fifth domain of warfare.**

Digital Universe

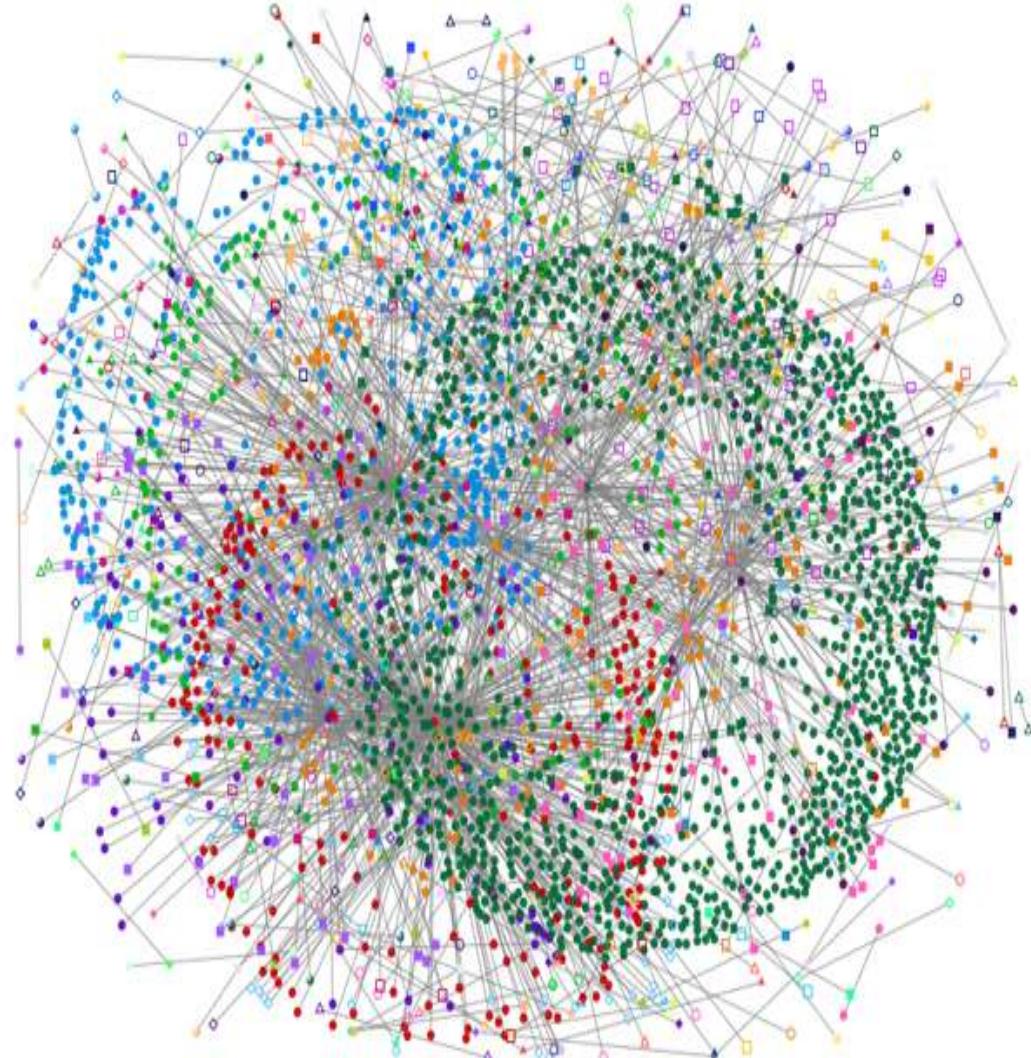


The Power of Social Graph



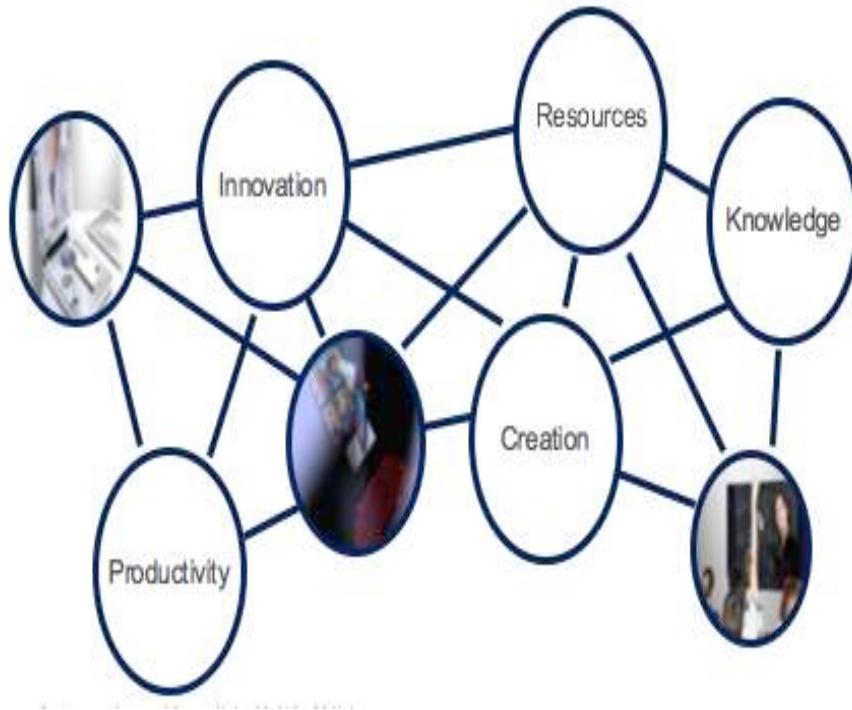
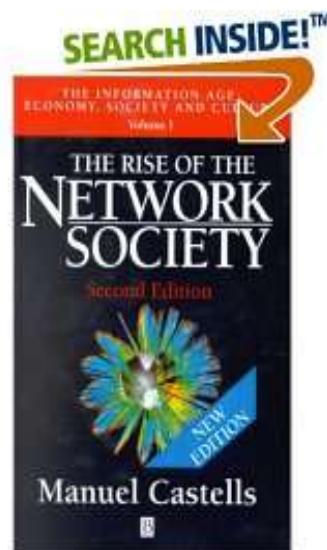
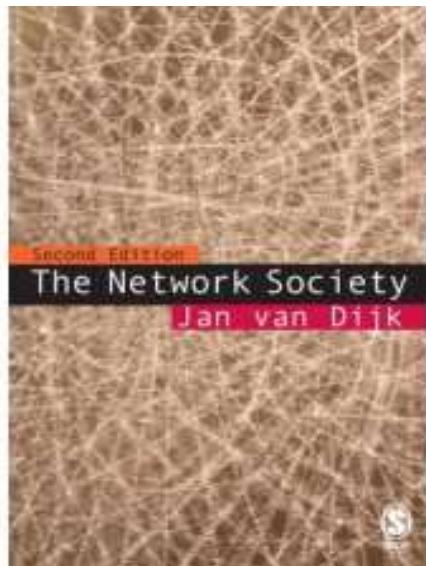
©LiquidLearn 2011

www.ValYouCasting.com



Networked Society

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

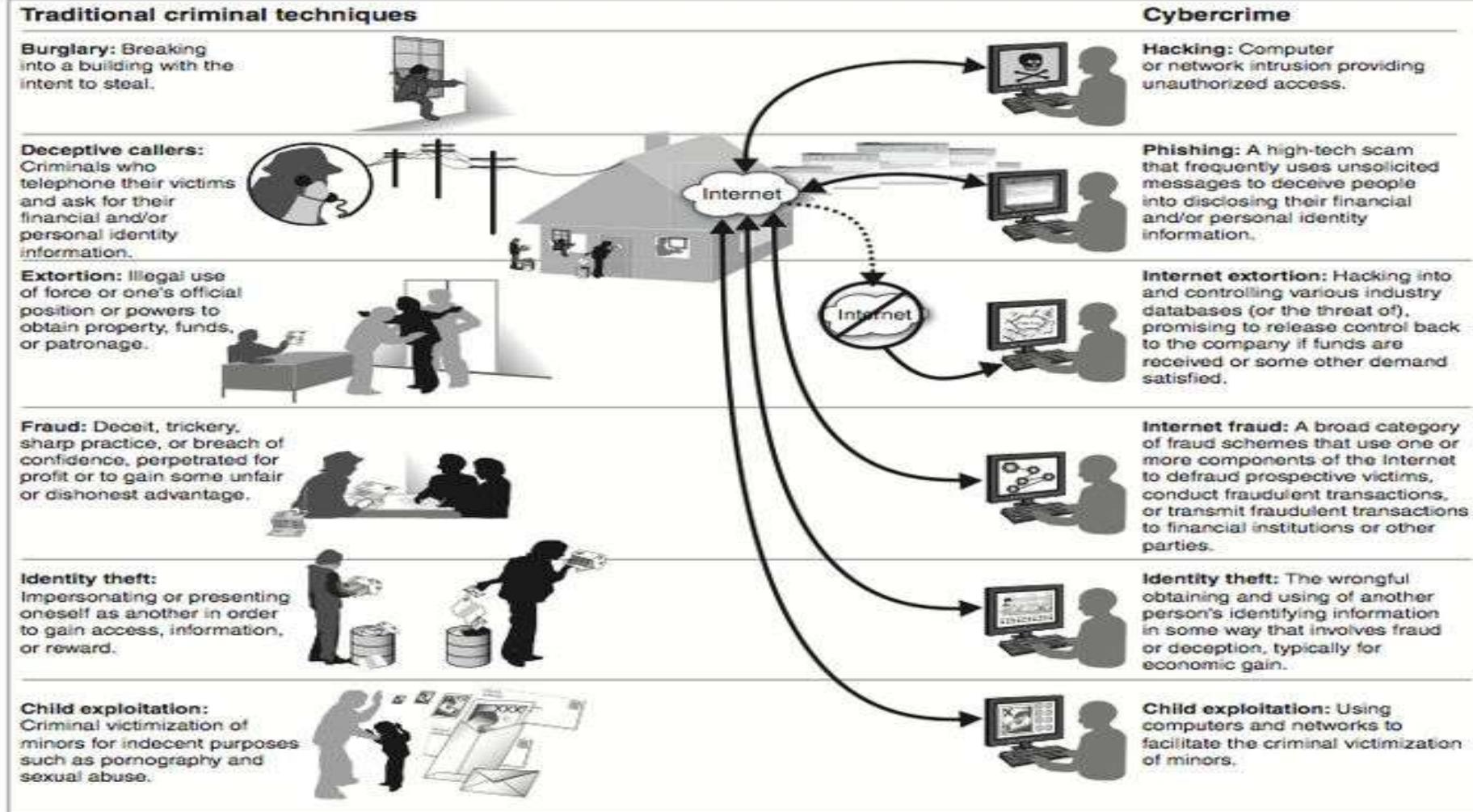


In the networked society people, knowledge, devices, and information are networked for the growth of society, life and business.

Traditional vs Cyber (crime)

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

Figure 1: Comparison between Traditional Criminal Techniques and Cybercrime



Klasifikasi Cybercrime

Principles of Cybercrime

Jonathan Clough

- 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 is more 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

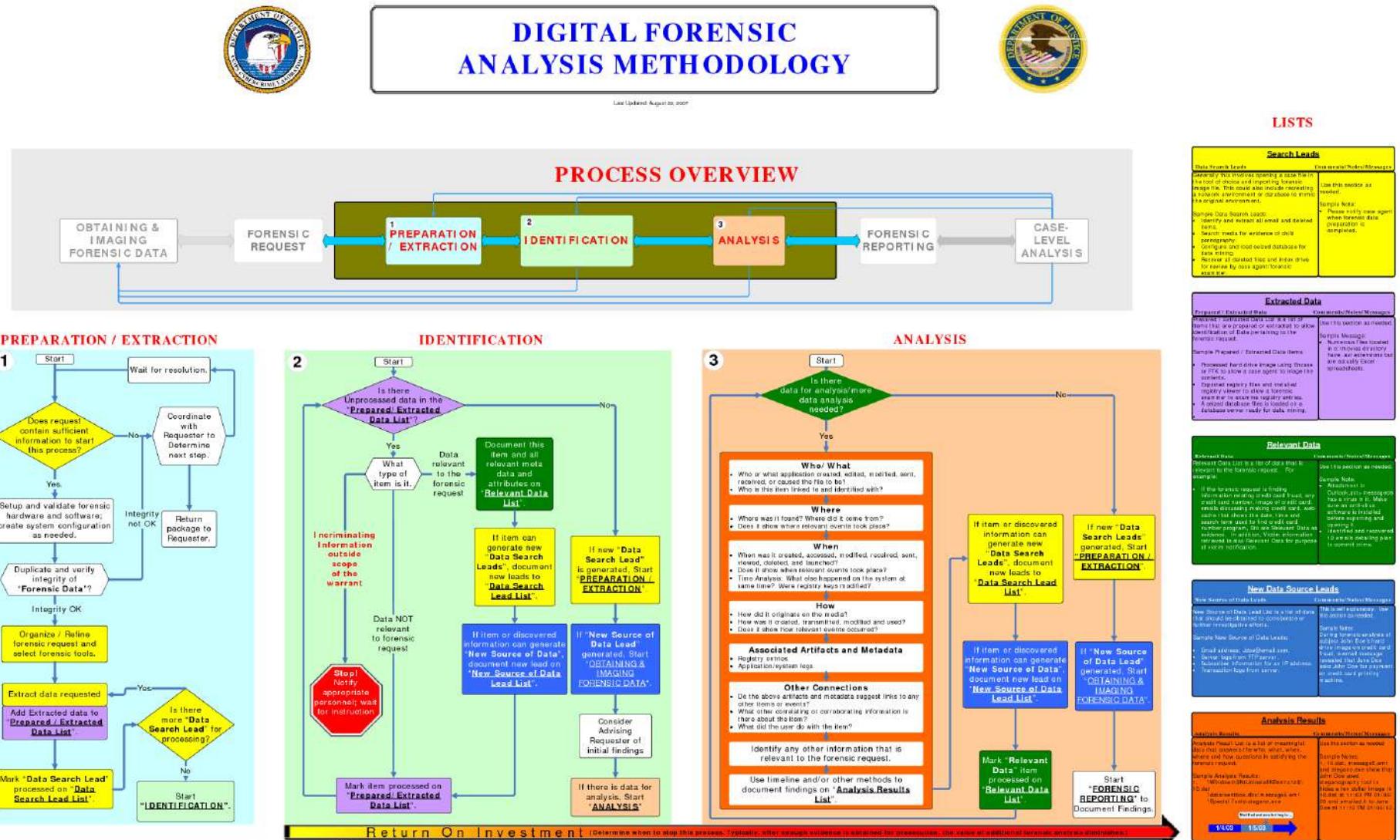
- Alat bukti yang sah dalam bentuk petunjuk sebagaimana dimaksud dalam Pasal 188 ayat (2) Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana, khusus untuk tindak pidana korupsi juga dapat diperoleh dari :
 - a. alat bukti lain yang berupa informasi yang diucapkan, dikirim, diterima, atau disimpan 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	<p>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.</p>																			
		<p>Kasus:</p> <ul style="list-style-type: none"> • 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 kirim dokumen WA. • Si B menggunakan data yang ada pada dokumen NIK/KK untuk melakukan registrasi kartu SIM CARD Prabavar 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. <p>Si A dan Si B kemudian ditangkap untuk dimintai pertanggungjawabannya terhadap penggunaan NIK/KK yang tidak sah 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.</p> <p>Bukti apa saja yang harus disiapkan agar pidana Pasal 35 UU ITE dpt diterapkan pada keduanya.</p>																			
Aspek	Unsur	<table border="1"> <thead> <tr> <th colspan="2">Analisa Kasus dan Bukti</th> </tr> <tr> <th>Perbuatan</th><th>Bukti yg harus didapat/dicari ?</th></tr> </thead> <tbody> <tr> <td>dengan sengaja</td><td>dengan sengaja menggunakan dokumen untuk registrasi</td><td>keberadaan dokumen serta history transaksi registrasi dengan dokumen tsb.</td></tr> <tr> <td>tanpa hak</td><td>tanpa hak memiliki dan menggunakan dokumen</td><td>Keberadaan file dokumen pada device milik tersangka</td></tr> <tr> <td>manipulasi, penciptaan, perubahan, penghilangan, pengrusakan</td><td>manipulasi registrasi dengan memasukkan Nama, NIK, KK tanpa hak</td><td>History registrasi dengan data yang termuat pada dokumen yang dimiliki tersangka</td></tr> <tr> <td>informasi elektronik dan/atau dokumen elektronik</td><td>informasi elektronik dan/atau dokumen elektronik berupa data KK dan NIK</td><td>Dokumen yang berisi NIK dan KK</td></tr> <tr> <td>agar informasi dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik</td><td>agar informasi dan/atau dokumen elektronik tersebut dianggap seolah-olah data yang otentik, untuk kepentingan registrasi Sim Card</td><td>History registrasi yang sukses serta efek lain dari keberhasilan registrasi yang didapat oleh tersangka.</td></tr> </tbody> </table>	Analisa Kasus dan Bukti		Perbuatan	Bukti yg harus didapat/dicari ?	dengan sengaja	dengan sengaja menggunakan dokumen untuk registrasi	keberadaan dokumen serta history transaksi registrasi dengan dokumen tsb.	tanpa hak	tanpa hak memiliki dan menggunakan dokumen	Keberadaan file dokumen pada device milik tersangka	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	informasi elektronik dan/atau dokumen elektronik	informasi elektronik dan/atau dokumen elektronik berupa data KK dan NIK	Dokumen yang berisi NIK dan KK	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.
Analisa Kasus dan Bukti																					
Perbuatan	Bukti yg harus didapat/dicari ?																				
dengan sengaja	dengan sengaja menggunakan dokumen untuk registrasi	keberadaan dokumen serta history transaksi registrasi dengan dokumen tsb.																			
tanpa hak	tanpa hak memiliki dan menggunakan dokumen	Keberadaan file dokumen pada device milik tersangka																			
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																			
informasi elektronik dan/atau dokumen elektronik	informasi elektronik dan/atau dokumen elektronik berupa data KK dan NIK	Dokumen yang berisi NIK dan KK																			
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.																			
Tujuan																					

Forensika Digital



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

Barang bukti adalah benda yang bergerak atau tidak bergerak, yang benwujud maupun yang tidak berwujud yang mempunyal hubungan dengan tindak pidana yang terjadi.

Pasal 39 ayat (1) KUHAP

1. Menguatkan kedudukan alat bukti yang sah (Pasal 184 ayat [1] KUHAP)

2. Mencari dan menemukan kebenaran materill atas perkara sidang yang ditangani

3. Setelah barang bukti menjadi penunjang alat bukti yang sah maka barang bukti tersebut dapat menguatkan keyakinan hakim atas putusan yang didakwakan JPU.

1. benda atau tagihan tersangka atau terdakwa yang seluruh atau sebagian diduga diperoleh dari tindakan pidana atau sebagai hasil dari tindak pidana;

2. benda yang telah dipergunakan secara langsung untuk melakukan tindak pidana atau untuk mempersiapkannya;

3. benda yang digunakan untuk menghalang-halangi penyelidikan tindak pidana;

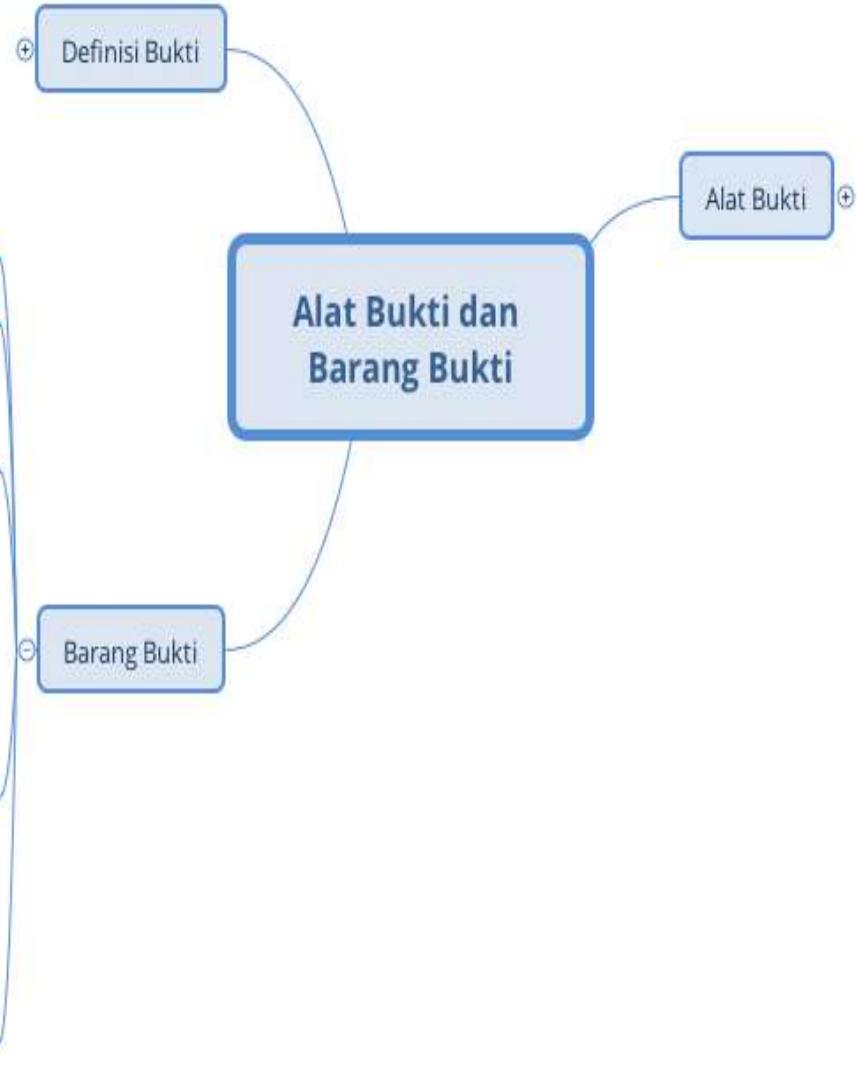
4. benda yang khusus dibuat atau diperuntukkan melakukan tindak pidana;

5 benda lain yang mempunyal hubungan langsung dengan tindak pidana yang dilakukan,

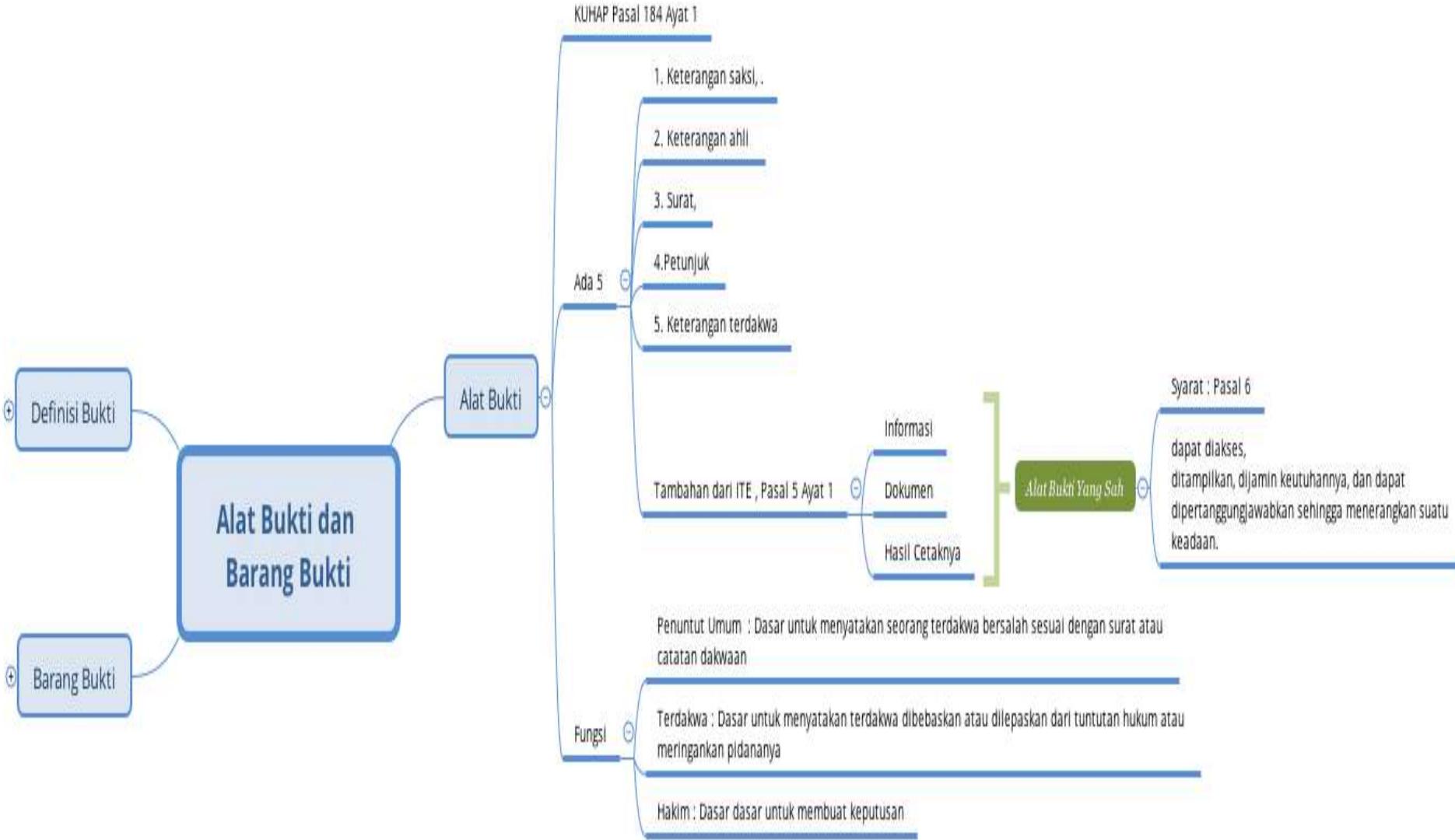
Witness

Tools

5 The Role of Evidence

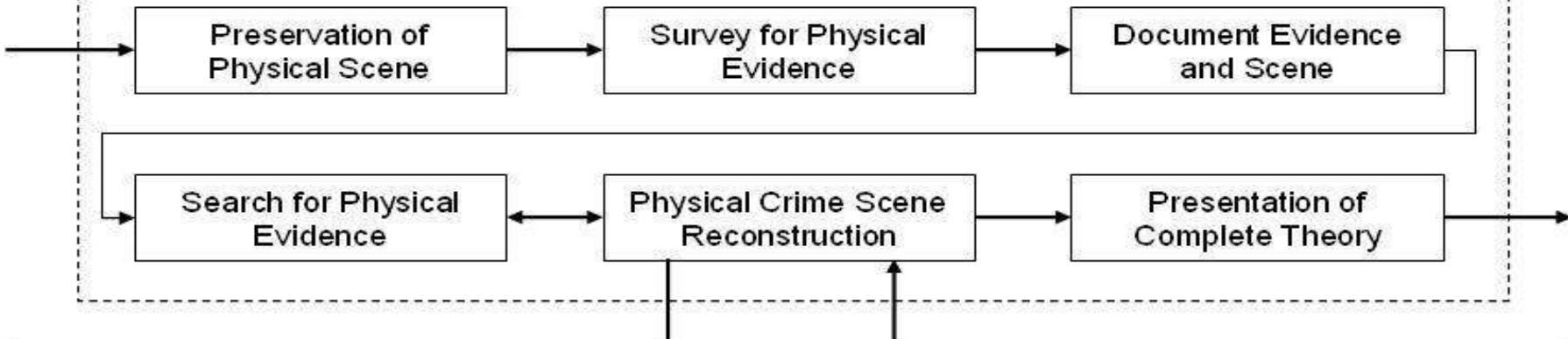


Alat Bukti

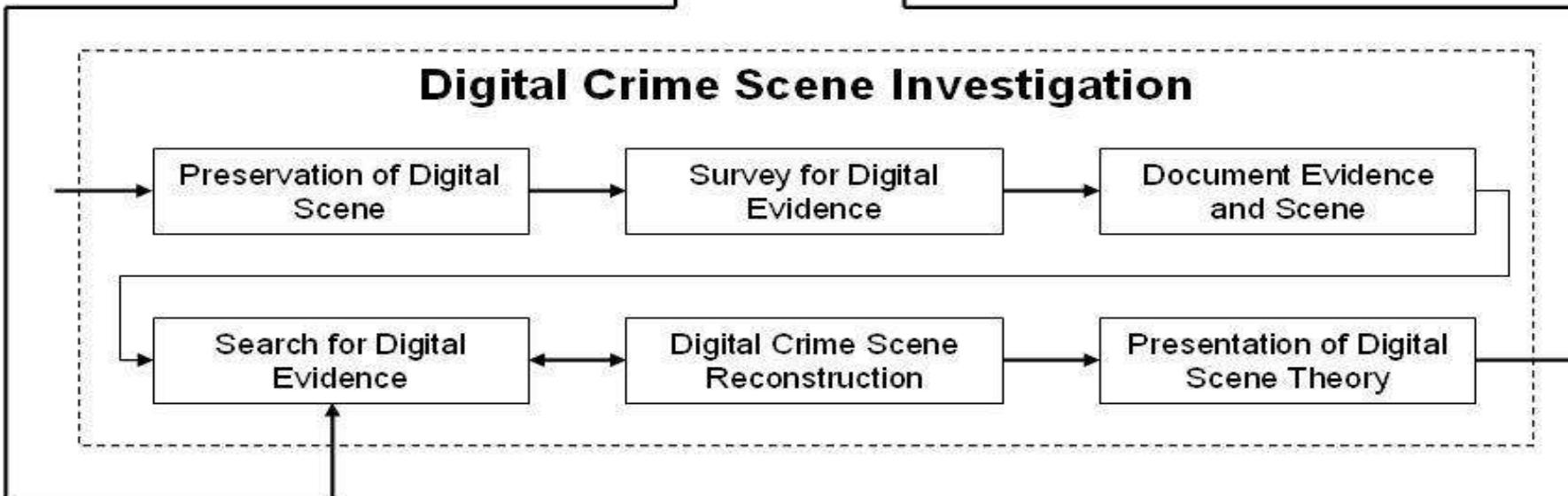


Physical + Digital Investigation

Physical Crime Scene Investigation

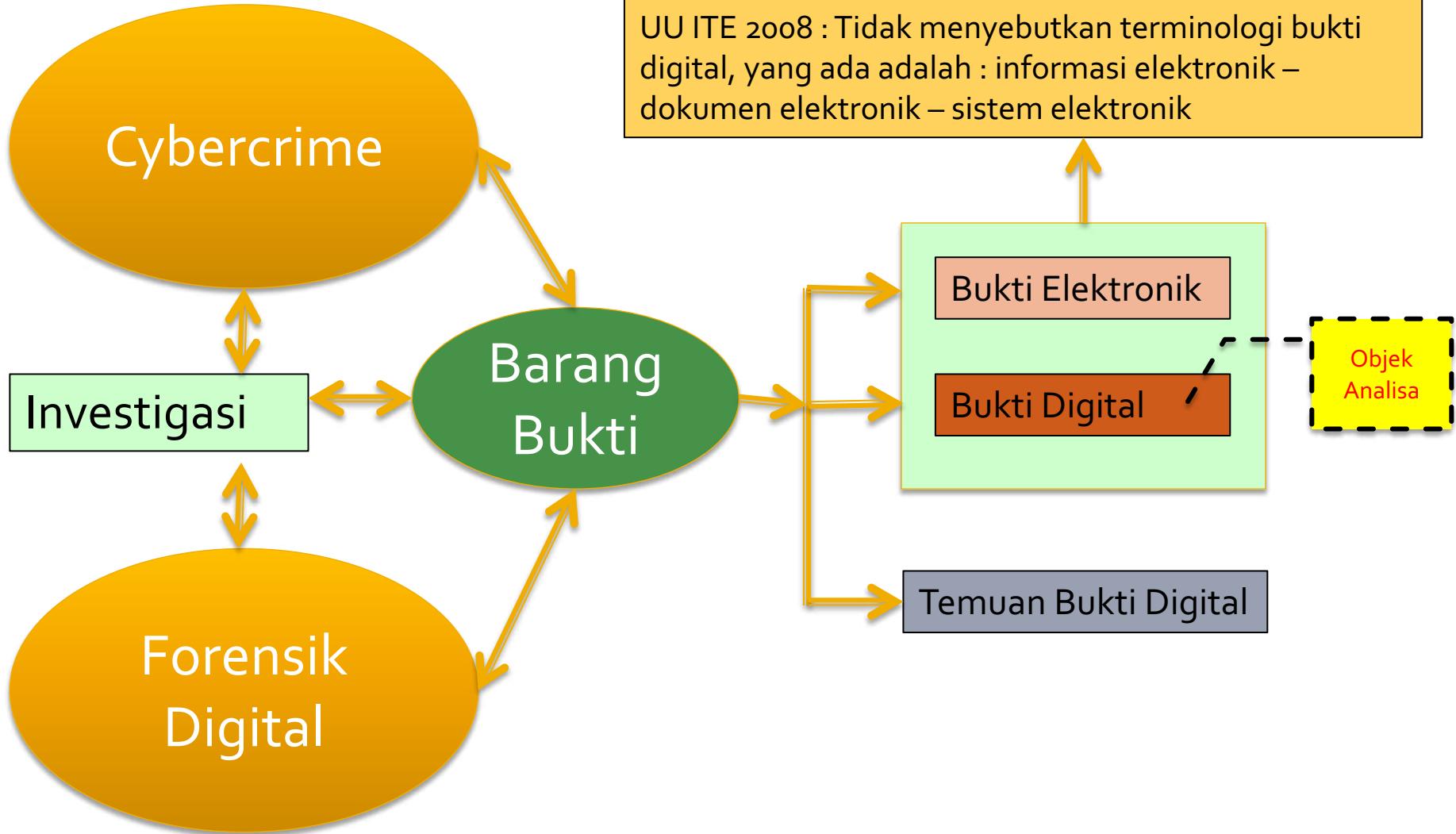


Digital Crime Scene Investigation



Bukti Digital

Terminologi



Bukti Digital

Terminologi

Bukti Elektronik

Bukti Digital

Temuan Bukti Digital

Multimedia File

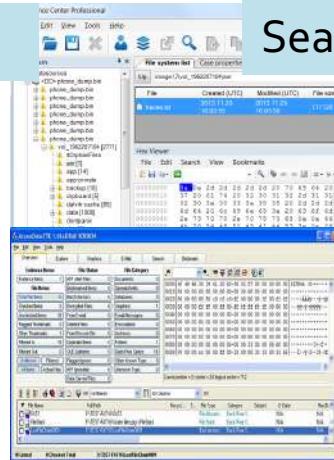
Audio, Image, Video,

Analisa Orisinalitas, Fakta

Offline



Akuisisi dan Imaging

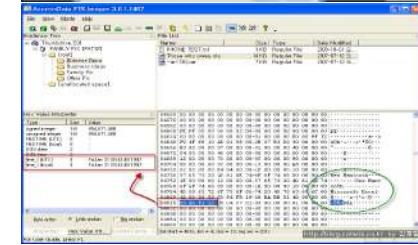
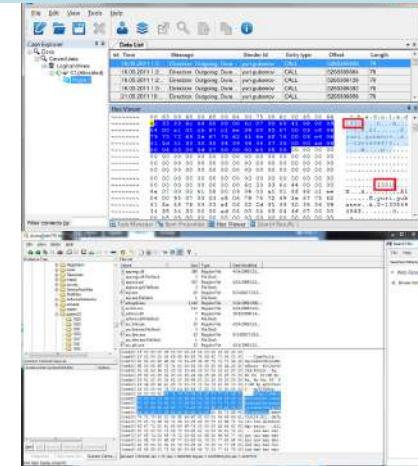
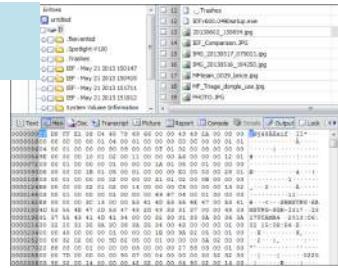


Searching - Eksplorasi dan Analisa

Online



Capture, record, log



Digital Evidence

Copyright CHFI ECCouncil

Characteristics of Digital Evidence

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



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

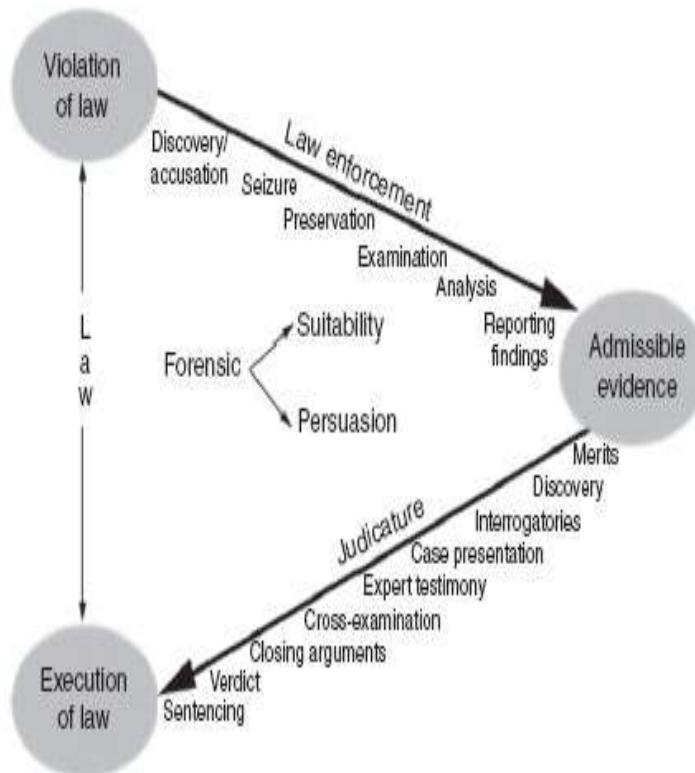
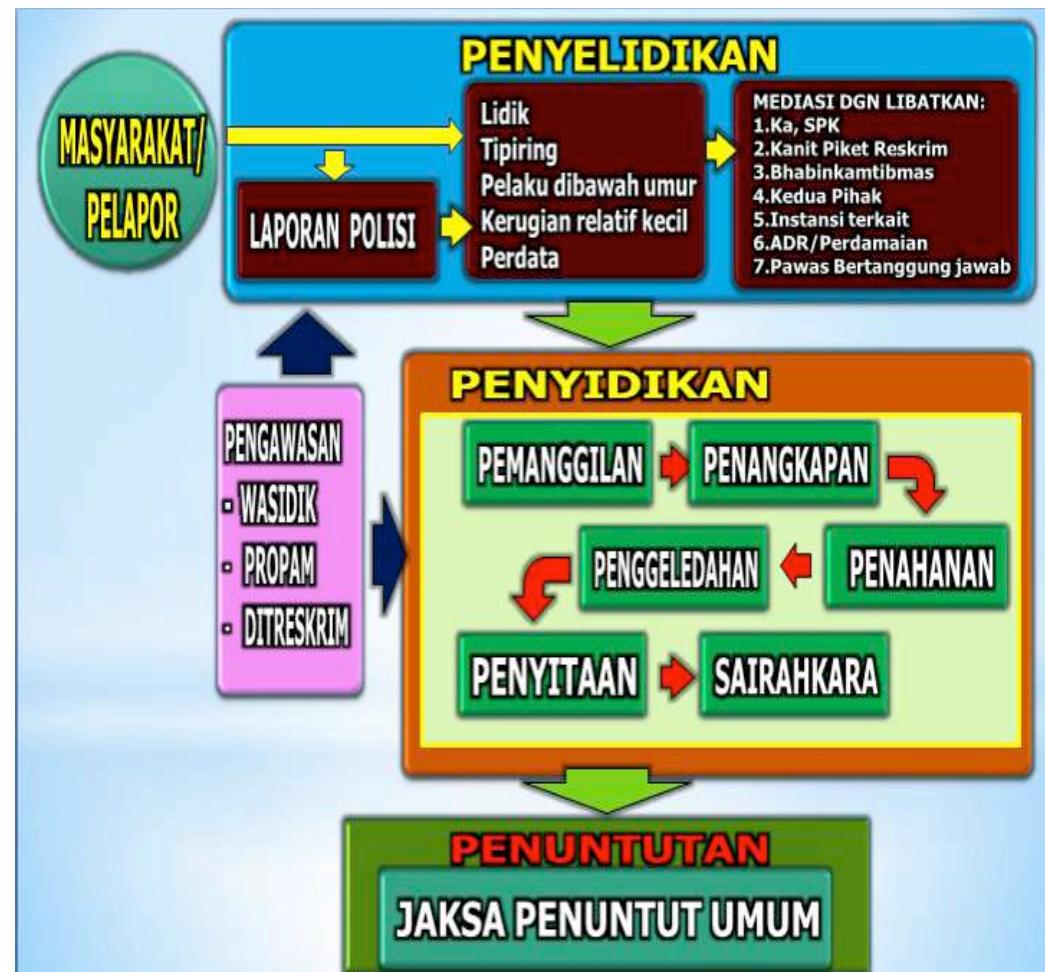
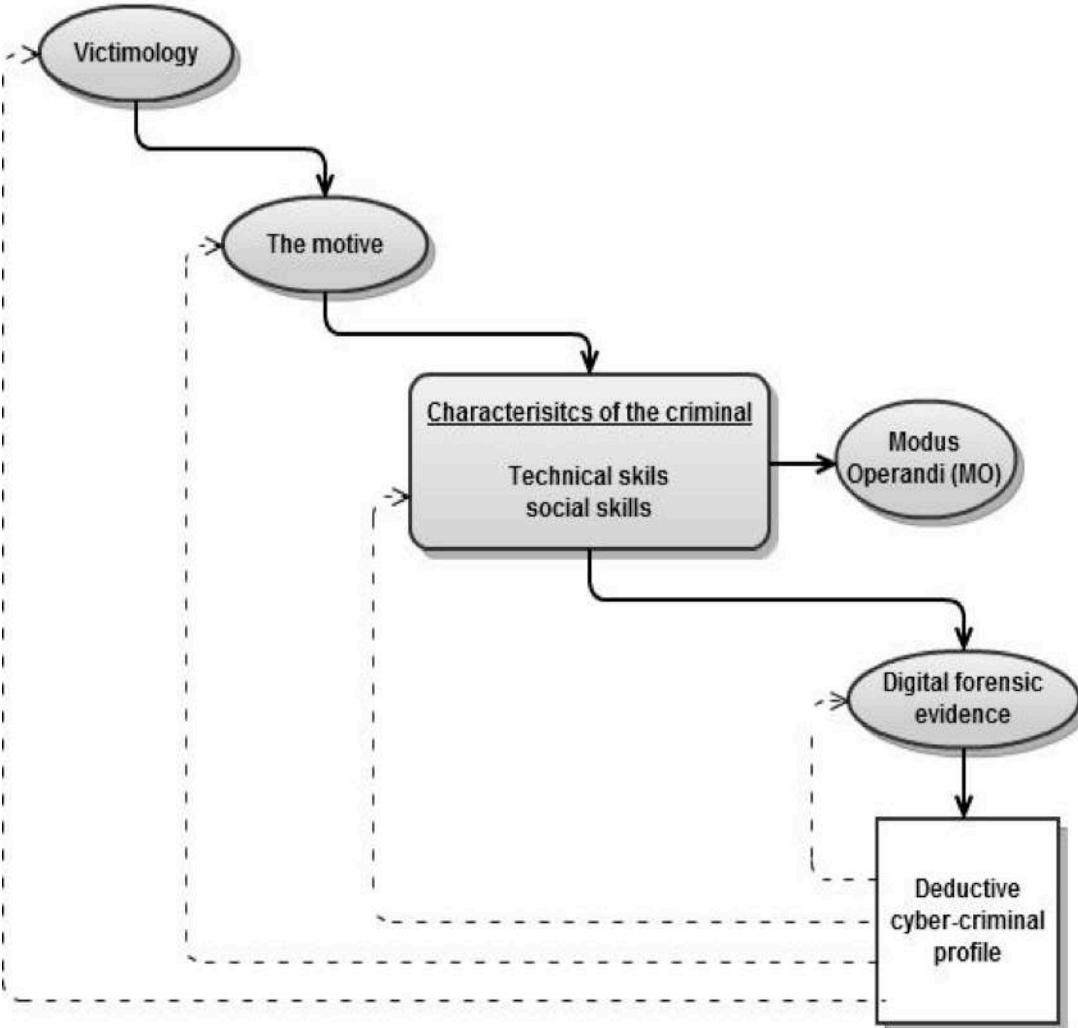


FIGURE 3.1

Overview of case/incident resolution process.



Profiling



HOW TO CRIME ANALISYS
FOR
Digital Forensic

www.ilmuforensikadigital.blogspot.com | ahmad.subki1992@gmail.com

the scenarios
menaraskan ulang kejadian secara berurut, sehingga dapat menggambarkan bagaimana peristiwa tersebut terjadi

1

the law
petakkan aspek hukum dan aturan apa saja yang dilanggar ketika melakukan kejadian tersebut.

2

who is liable?
siapa saja yang terlibat dalam kasus kejadian tersebut dan apa perannya

3

motive & modus
deskripsikan tujuan pelaku melakukan kejadian tersebut dan jelaskan apa saja langkah-langkah yang dilakukan untuk melancarkan kejahatannya

4

digital evidence
jelaskan apa saja barang bukti digital maupun elektronik yang ditemukan dan dimana tempat ditemukannya

5

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.



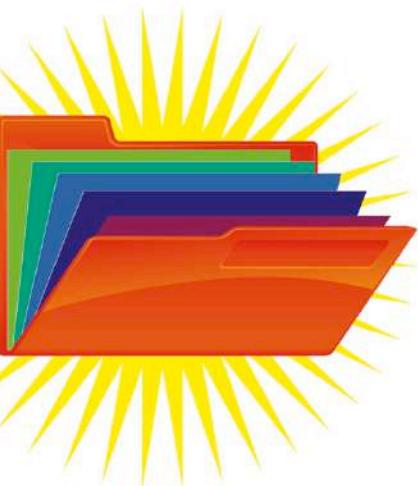
Connections Discovered

By off-the-shelf servers running Bolero™

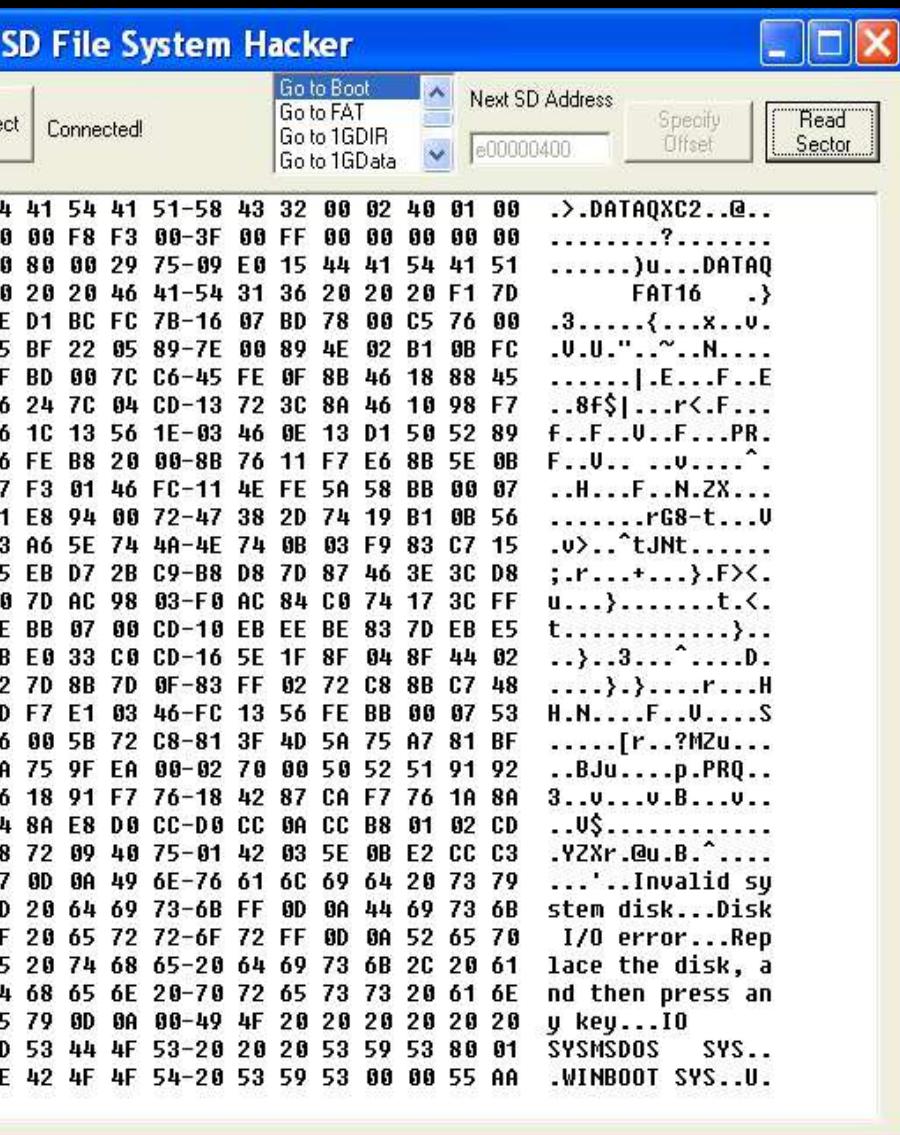


Suspect/Possibly Incriminating Files

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

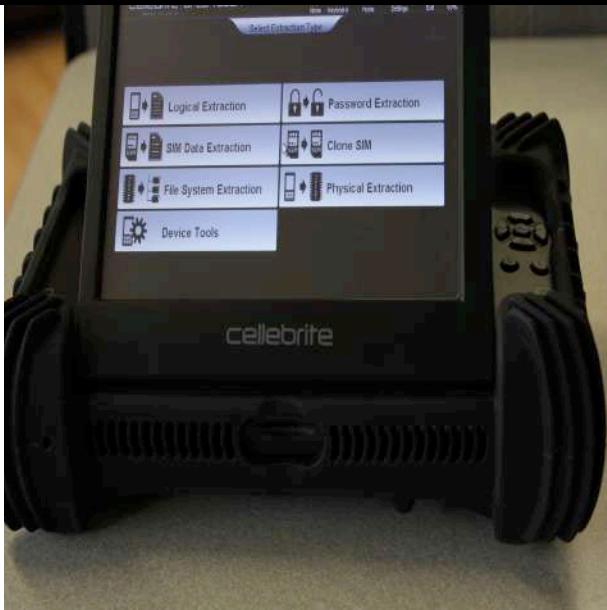
Sector = 0x200 => 512

Sector per Cluster = 8

1 Cluster = 512 * 8 = 4096

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF	
0000h:	EB	52	90	4E	54	46	53	20	20	20	20	00	02	0B	00	00	ëR.NTFS	
0010h:	00	00	00	00	00	F8	00	00	00	00	00	00	00	00	00	00ø.....	
0020h:	00	00	00	00	80	00	80	00	1F	AF	00	00	00	00	00	00e.e..N.....	
0030h:	04	00	00	00	00	00	00	00	E1	04	00	00	00	00	00	00á.....	
0040h:																	ö.....ú."14IØ(
0050h:																ú3ÄžDñ. uhA.	
0060h:	0x04 => 4 First Cluster of MFT								0x04 E1 First Cluster of MFT Mirror								..hf.È^...f.>..N	
0070h:																	TFSu.'A»"Uí.r..ú	
0080h:	55	AA	75	06	F7	C1	01	00	75	03	E9	D2	00	1E	83	EC	U"u.+Á..u.éØ..fi	
0090h:	18	68	1A	00	B4	48	8A	16	0E	00	8B	F4	16	1F	CD	13	.h..'HŠ...<8..f.	
00A0h:	9F	83	C4	18	9E	58	1F	72	E1	3B	06	0B	00	75	DB	A3	ÝfA.žX.rá;...u0£	
00B0h:	0F	00	C1	2E	0F	00	04	1E	5A	33	DB	B9	00	20	2B	C8	..Á.....Z30¹. +È	
00C0h:	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	06	16	00	E8	fý.....žÄy...è	
00D0h:	40	00	2B	C8	77	EF	B8	00	BB	CD	1A	66	23	C0	75	2D	@.+Èwi..»í.f#Åu-	
00E0h:	66	81	FB	54	43	50	41	75	24	81	F9	02	01	72	1E	16	f.ÙTCPAu\$.ù...r..	
00F0h:	68	07	BB	16	68	70	0E	16	68	09	00	66	53	66	53	66	h.»hp..h..fsfsf	
0100h:	55	16	16	16	68	B8	01	66	61	0E	07	CD	1A	E9	6A	01	U...h..fa..í.éj.	
0110h:	90	90	66	60	1E	06	66	A1	11	00	66	03	06	1C	00	1E	..f`..f;..f.....	
0120h:	66	68	00	00	00	00	66	50	06	53	68	01	00	68	10	00	fh....fP.Sh..h..	
0130h:	B4	42	8A	16	0E	00	16	1F	8B	F4	CD	13	66	59	5B	5A	'BŠ.....<8í.fY[Z	
0140h:	66	59	66	59	1F	0F	82	16	00	66	FF	06	11	00	03	16	fYfY....fý.....	
0150h:	0F	00	8E	C2	FF	0E	16	00	75	BC	07	1F	66	61	C3	A0	..žÄy...uñ..faÄ	
0160h:	F8	01	E8	08	00	A0	FB	01	E8	02	00	EB	FE	B4	01	8B	ø.è.. g.è..éþ'..<	
0170h:	F0	AC	3C	00	74	09	B4	0E	BB	07	00	CD	10	EB	F2	C3	ð-<.t.'..»..í.éðÄ	
0180h:	0D	0A	41	20	64	69	73	6B	20	72	65	61	64	20	65	72	..A disk read er	
0190h:	72	6F	72	20	6F	63	63	75	72	72	65	64	00	0D	0A	42	ror occurred...B	
01A0h:	4F	4F	54	4D	47	52	20	69	73	20	6D	69	73	73	69	6E	OOTMGR is missin	
01B0h:	67	00	0D	0A	42	4F	4F	54	41	0xAA55 Boot Sector Signature								g...BOOTMGR is compressed...Pres
01C0h:	6F	6D	70	72	65	73	73	65	6	0xAA55 Boot Sector Signature								s Ctrl+Alt+Del t
01D0h:	73	20	43	74	72	6C	2B	41	61	0xAA55 Boot Sector Signature								o restart.....
01E0h:	6F	20	72	65	73	74	61	72	74	6D	6A	66	66	66	66	66é.²ø..Uä	
01F0h:	00	00	00	00	00	00	00	00	80	9D	B2	CA	00	00	55	AA		

Hardware dan Software



Digital Intelligence



X-Ways



TABLEAU
Solutions for the Digital Evidence Lifecycle™



SiQuest
EVERY BIT COUNTS

Kesiapan APH



Forensik Digital di BPKP



www.bpkp.go.id/investigasi/konten/2207/Pedoman-Pengumpulan-dan-Pengevaluasian-Bukti-Dokumen-Elektronik

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

