

PERKEMBANGAN INTERNET PADA GENERASI MUDA DI INDONESIA DENGAN KAITAN UNDANG-UNDANG ITE YANG BERLAKU

Said Akmala¹

¹Jurusan Magister Teknik Informatika Fakultas Teknologi Industri Universitas Islam Indonesia
Jalan Kaliurang KM.14,5 Sleman, Yogyakarta 55584
Email: kirimemailsaid@gmail.com

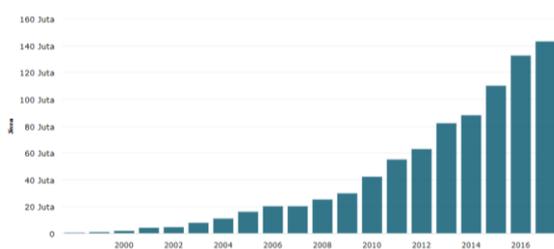
Abstrak

Perkembangan internet di Indonesia semakin meningkat dari tahun ke tahun, hal ini membuktikan bahwa internet memiliki peran yang penting terhadap berbagai aspek yang ada. Awalnya internet dikembangkan dan digunakan untuk kepentingan militer di abad 19, namun perkembangan dan kebutuhan akan teknologi terus menuntut internet digunakan di berbagai banyak sektor seperti perdagangan, sosial, hingga ke sistem pemerintahan. Di Indonesia, internet sudah banyak digunakan oleh berbagai kategori usia pengguna mulai dari anak-anak sampai usia lanjut. Padahal seperti yang kita ketahui bersama internet sendiri memiliki banyak sisi positif namun juga banyak hal negatif yang perlu diwaspadai oleh *user* atau penggunanya. Keterkaitan antara keamanan terhadap data menjadi salah satu hal yang paling penting, karena data merupakan komponen utama harus dijaga dengan baik. Penyalahgunaan data tentu akan menimbulkan banyak kerugian mulai dari pemalsuan data hingga kehilangan data. Paper ini membahas mengenai sisi positif dan negatif internet khususnya bagi generasi muda di Indonesia yang dikaitkan dengan kasus pelanggaran hukum undang-undang ITE dengan beberapa konsep chain of custody.

Kata kunci: *internet, UU ITE, chain of custody, cybercrime*

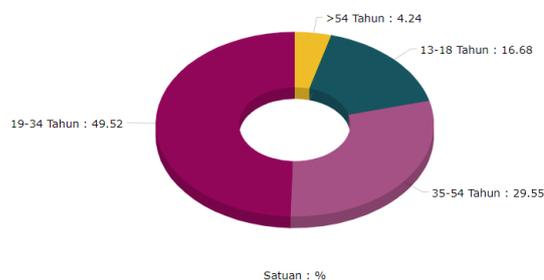
1. PENDAHULUAN

Kemajuan teknologi membuat perkembangan internet terus meningkat, kebutuhan informasi dan pengetahuan juga menjadi faktor perkembangannya. Di Indonesia pengguna internet terus meningkat, berikut data pertumbuhan internet di Indonesia :



Gambar 1. Pengguna Internet di Indonesia (1998-2017)

Kategori pengguna internet di Indonesia berdasarkan kelompok usia pada tahun 2017 juga beragam, dari usia 13-18 tahun (16.68 %), 19-34 tahun (49.52%), 35-54 (29,55%), >54 tahun (4.24%) seperti data pada Gambar 2. Presentase tersebar pada data tersebut ada di usia 19-34 yaitu sebesar 49.52%, usia tersebut termasuk ke dalam usia pemuda/ generasi muda. Tentu hal ini sudah selayaknya menjadi perhatian agar nantinya kelompok usia pemuda bisa memaksimalkan manfaat internet dengan baik.

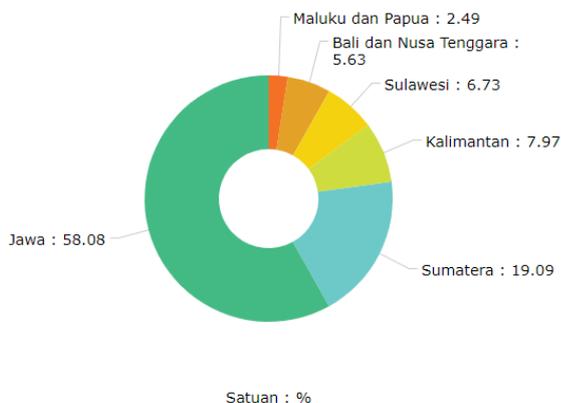


Gambar 2. Pengguna Internet Berdasarkan Kelompok Usia (2017)

Keamanan dalam penggunaan dan pemanfaatan internet merupakan hal yang wajib diketahui oleh penggunanya, tidak sedikit yang menyalahgunakan internet untuk melakukan berbagai kejahatan ilegal yang tentu akan melanggar hukum. Di Indonesia sendiri penggunaan internet sudah diatur dalam Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Dalam mengungkap kasus kejahatan internet banyak sekali metode yang digunakan, salah satunya adalah langkah *chain of custody* yaitu kronologis pendokumentasian barang bukti, dari mulai di temukan di TKP hingga penduplikasian dan penyimpanannya baik secara fisik ataupun digital. Tentunya langkah tersebut harus dilakukan oleh seorang yang ahli dalam bidang tersebut.

2. PENGGUNA INTERNET DI INDONESIA

Pengguna internet di Indonesia sangat beragam, namun penyebarannya masih terpusat dan terbesar di Pulau Jawa (58,08%), disusul Sumatra (19,09%), Kalimantan (7,97%), Sulawesi (6,73%), Bali dan Nusa Tenggara (5,63%), Maluku dan Papua (2,49%).



Gambar 3. Komposisi Pengguna Internet di Indonesia Menurut Pulau (2017)

Dari data diatas, diperlukan adanya perataan pengguna internet yang lebih luas terutama pada lokasi/ pulau yang masih tertinggal.

2.1 Manfaat dan Dampak Internet

Tabel 1. Manfaat dan Dampak Internet

Aspek	Manfaat	Dampak
Learning	Sumber informasi yang sangat luas	Informasi yang salah, data tidak valid, sumber tidak jelas
Thinking	Banyak terdapat argument, kritik, penyelesaian masalah	Salah Paham, Perubahan Moral
Motivation	Banyak pengalaman	Adiktif
Inspiration	Kepahlawanan, Ide, Inspirasi	Salah mengambil sumber inspirasi
Social Life	Mendekatkan yang jauh	Penyalahgunaan data pribadi
Investigating	Menemukan hal menarik orang lain	Menemukan data pribadi orang lain
Entertainment	Hiburan	Pornografi, Pembunuhan, Online Risk

Bagaikan dua mata pisau, internet memiliki banyak sisi positif dan negatif yang menuntut penggunaannya agar lebih bijak dalam menggunakannya. Perhatian akan pentingnya penggunaan internet bagi kalangan remaja di Indonesia sendiri masih jauh tertinggal dari negara maju seperti Amerika yang sudah menerapkan kebijakan dan kontrak antara orang tua dan anaknya dalam kaitannya penggunaan internet yang lebih aman. Mereka sangat memperhatikan masalah mengenai keamanan data pribadi, anak-anak tidak diperbolehkan memberikan data pribadi kepada orang lain dan dibuat secara tertulis layaknya perjanjian sebuah kontrak antara orang tua dan anak.

Kepedulian mengenai internet sudah selayaknya diterapkan di Indonesia, karena tidak sedikit kasus pelanggaran hukum tentang penggunaan teknologi. Walaupun sudah diatur oleh undang-undang ITE, masih banyak kasus yang terjadi akibat pelanggaran yang dilakukan oleh tersangka penyalahgunaan internet itu sendiri. Asian School of Cyber Laws sendiri membagi kasus kejahatan dan penyalahgunaan teknologi menjadi 69 jenis kejahatan yang berbeda yaitu :

Tabel 2. Jenis Kejahatan Cyber

1	Anonymizer	36	Impersonation
2	ARP cache poisoning	37	Joe - Job
3	Backdoor	38	Key stroke Logging
4	Bacscatter	39	Logic Bomb
5	The Blues-Bluebugging, Bluejacking and Bluesnarfing	40	Phishing & Spoofing attacks
6	Buffer overflow	41	Piggy backing
7	Bullying in Cyberspace	42	Piracy of Software
8	Click fraud	43	Pod Slurping
9	Computer trespass	44	Poisoning the Source
10	Cookie Manipulation	45	Pornography
11	Copyright infringement	46	robotstxt file
12	Crap-flooding	47	Port scanning
13	Cyber Stalking	48	Rootkits
14	Cyber Terrorism	49	Salami Theft
15	Cyber Warfare	50	Sale of Illegal Articles
16	Data Diddling	51	Scavenging
17	Data Leakage	52	Smishing
18	Defamation	53	Social Engineering
19	DOS / DDOS	54	Spambot
20	DNS poisoning	55	SQL Injection
21	Easter Eggs	56	Stalware
22	Email Spoofing	57	Time Bomb
23	Encryption use by terrorists	58	Trojan
24	eShoplifting	59	URL Manipulation
25	Financial Crimes	60	Virus Attack
26	Fire Sale	61	Web defacement
27	Fire Walking	62	Vishing
28	Footprinting	63	Wire - Tapping
29	Fraud	64	Worm
30	Online Gambling	65	XSS Attack
31	Google based hacking	66	YK
32	Griefers	67	Zero Day Attack
33	Hactivism	68	Zeus
34	Hijacking	69	Zombie
35	Identity Fraud		

Dari jenis kejahatan yang banyak terjadi, Indonesia sudah mengatur melalui kebijakan Undang-undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik yang terdiri dari XIII BAB yang mengatur banyak aspek penggunaan teknologi mulai dari kebijakan hingga ketentuan denda dan pidana.

3. PELANGGARAN HUKUM ITE

Dari kasus yang dikutip pada <http://www.hukumonline.com/berita/baca/lt4fb47c35db7b0/penyebar-foto-palsu-korban-sukhoi-dijerat-uu-ite> tentang Penyebar Foto Palsu Korban Sukhoi

dapat dianalisa dengan menggunakan metode *chain of custody*, yaitu kronologis pendokumentasian barang bukti, dari mulai di temukan di TKP hingga penduplikasian dan penyimpanannya baik secara fisik ataupun digital yang sudah dilakukan oleh Kapolda Metro Jaya beserta jajarannya.

3.1 Analisa Kasus

Dari kasus diatas dapat diambil informasi yaitu :

- a. What : Penyalahgunaan Teknologi Informasi, Kasus : **“Penyebar Foto Palsu Korban Pesawat Sukhoi”**
- b. Who : Yogi Santani (*pelaku*), Mahasiswa asal Lampung
- c. When : Rabu, 9 Mei 2012
- d. Where : Menyebar foto palsu di jejaring sosial *Twitter*
- e. Why : Penyidik masih mendalami motif Yogi (*pelaku*), namun Yogi mengaku tidak memiliki niat jahat untuk menyakiti keluarga korban pesawat sukhoi
- f. How : Analisa Ahli : Yogi melakukan penyeditan foto korban pesawat sukhoi dengan menggunakan software tertentu sehingga terlihat foto tersebut benar-benar nyata, kemudian disebar di jejaring sosial *Twitter*

3.2 Analisa Aspek Hukum

Analisa kasus penyalahgunaan teknologi informasi yang sudah menjerat Yogi dengan Pasal 35 UU ITE menyebutkan “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”. Pasal 51 ayat (1) menyebutkan, “Setiap orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 tahun dan atau denda paling banyak Rp12 miliar”.

Dari aspek hukum diatas Yogi bisa dipidana maksimal 12 tahun penjara atau dengan paling banyak 12 miliar, namun itu tergantung keputusan hakim. Hingga kemarin malam (17/5/2012), penyidik belum melakukan penahanan karena Yogi dinilai cukup kooperatif karena Yogi langsung menyerahkan diri.

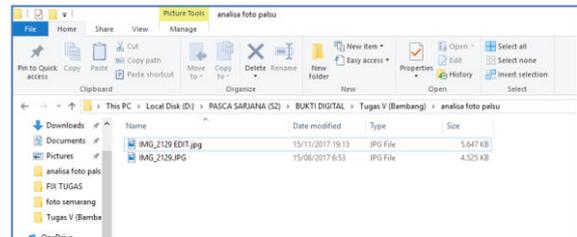
3.3 Analisa Aspek IT

Untuk mengungkap hasil dan Analisa foto palsu tersebut ada beberapa Teknik yang dapat dilakukan yaitu dengan cara melihat Details File dan Melakukan Analisa foto dengan software.

- a. Details File

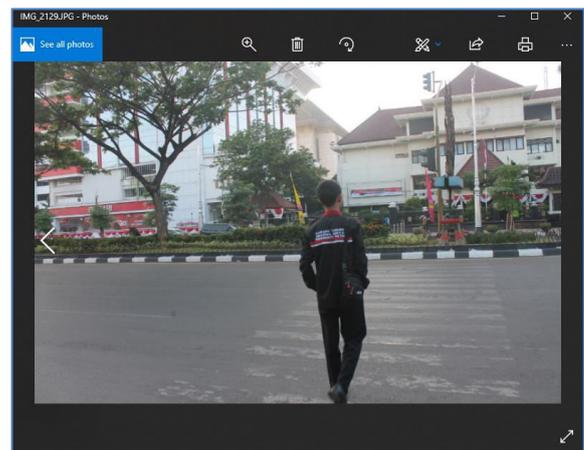
Kasus penyebar foto palsu tersebut apakah foto yang disebarakan pelaku benar-benar foto asli atau palsu bisa dibuktikan dengan melalui beberapa cara yaitu dengan melihat details file dari foto yang diunggahnya. Langkah-langkahnya adalah sebagai berikut :

- 1) Gunakan dua file (asli dan telah diedit) :

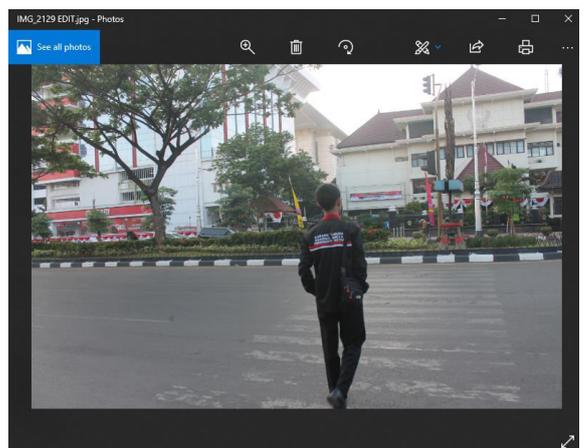


Gambar 4. File dasar analisa

Kedua file tersebut merupakan foto asli dan foto palsu (telah diedit) dengan hasil foto sebagai berikut:



Gambar 5. Foto IMG_2129.JPG



Gambar 6. Foto IMG_2129.EDIT.JPG

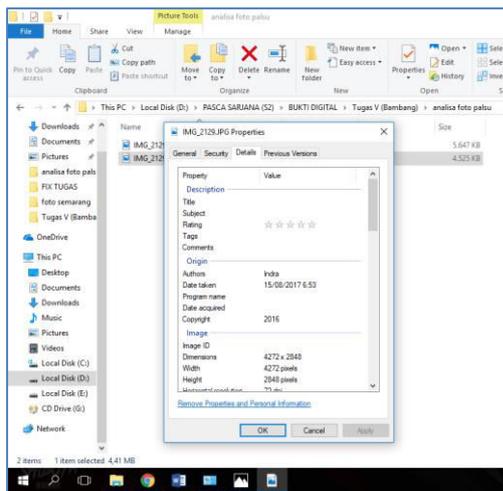
Keterangan : untuk melakukan penyujian perbedaan file foto asli dan telah diedit (palsu) penulis

menggunakan dan melakukan simulasi dengan foto sendiri.

- 2) Masuk ke properties lalu lihat details dari file tersebut :

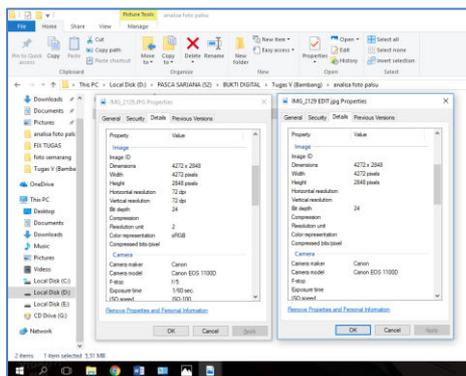
Dari kedua foto tersebut terlihat tidak ada perbedaan apapun antara foto yang asli dan yang telah diedit (palsu). Maka perlu dilakukan analisa details file tersebut, adapun langkahnya yaitu :

- a) Klik kanan file tersebut – properties – details :

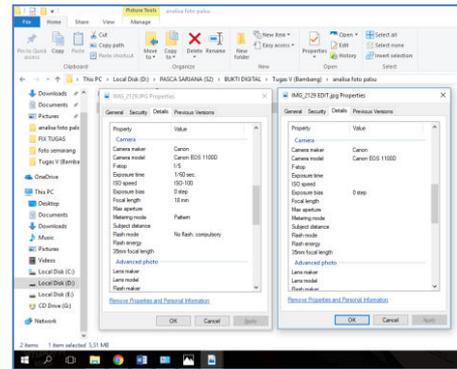


Gambar 7. Hasil Details File

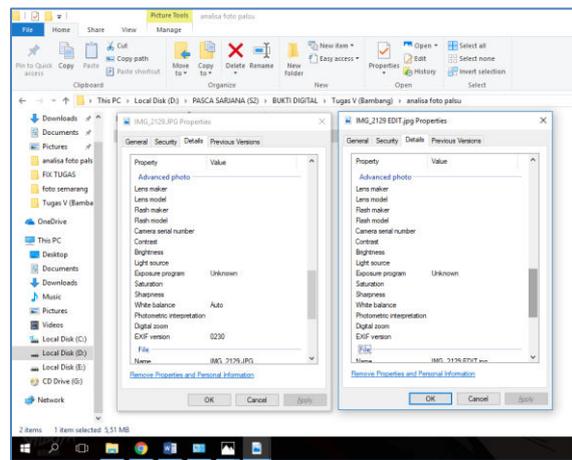
- b) Lakukan analisa dari details file tersebut dengan membacanya pada deskripsi details file tersebut. Berikut ini adalah hasil details file dari kedua file tersebut :



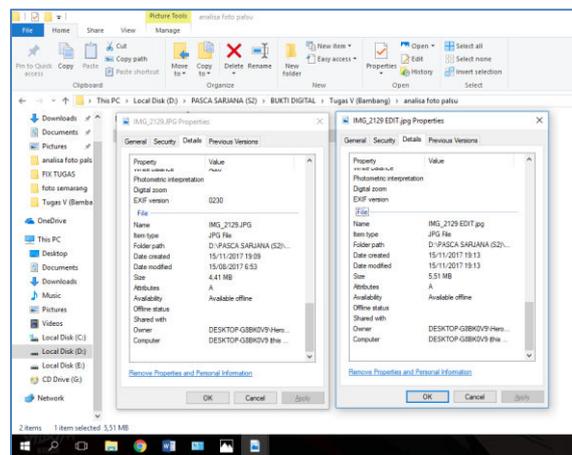
Gambar 8. Perbedaan di informasi image diatas



Gambar 9. Perbedaan di informasi camera diatas



Gambar 10. Perbedaan di informasi advanced photo diatas



Gambar 11. Perbedaan di informasi file diatas

Dari langkah analisa details file tersebut banyak sekali perbedaan deskripsi kedua file tersebut. Ini menandakan bahwa salah satu dari kedua file tersebut telah mengalami pengeditan atau perubahan. Namun langkah diatas hanya sebagai informasi dasar saja, untuk memutuskan file manakah yang telah diedit memerlukan suatu analisa yang lain, salah satunya adalah menggunakan software JPEGsnoop.

- b. Software JPEGsnoop

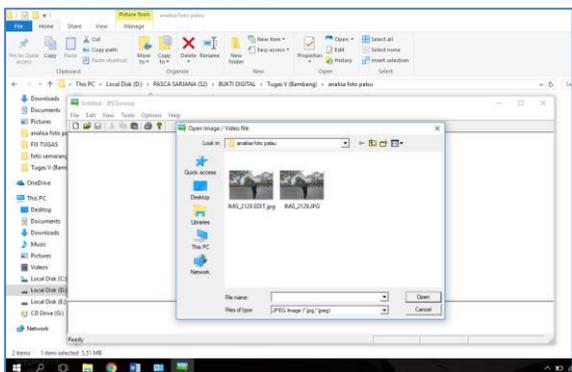
JPEGsnoop merupakan *software* yang bisa menganalisa dan menentukan apakah file tersebut

asli atau telah diedit (palsu). Adapun file yang dapat dilakukan analisa adalah :

- 1) Gambar : jpg, jpeg, crw, cr2, nef, orf, pef, dng
- 2) Video : .avi, .mov
- 3) Dokumen : .pdf, .thm

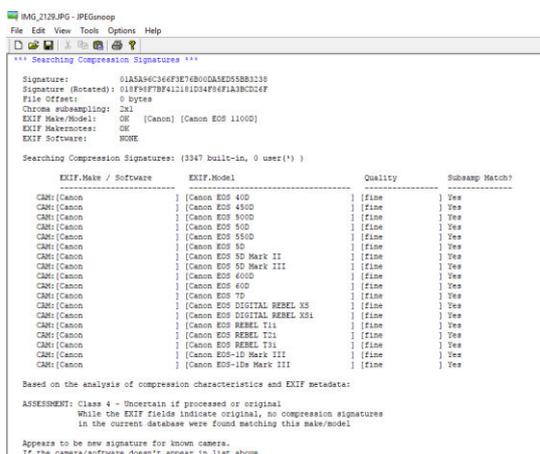
Mari kita lakukan analisa foto yang sudah dilakukan pada langkah details diatas sebagai berikut :

- 1) Jalankan software JPEGsnoop dan buka file yang akan dilakukan analisa :

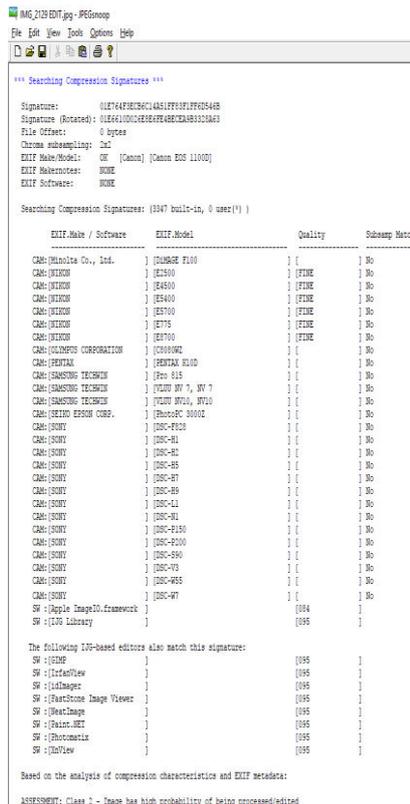


Gambar 12. File yang akan dianalisa

- 2) Tunggu program melakukan proses analisa dan berikut adalah hasil dari kedua file tersebut :



Gambar 13. Hasil Analisa File Asli



Gambar 14. Hasil Analisa File Palsu

Dari kedua hasil aplikasi JPEGsnoop diatas maka dapat disimpulkan :

- 1) file yang pertama adalah masuk ke dalam : CLASS 4
- 2) file yang kedua adalah masuk ke dalam : CLASS 2

Apabila file tersebut masuk kedalam klasifikasi Class 4 maka file tersebut bisa dikatakan asli dan apabila file tersebut masuk kedalam klasifikasi Class 2 maka file tersebut bisa dikatakan telah diedit (palsu). Selain dari hasil *class* tersebut kita bisa membaca deskripsi file. Apabila file tersebut asli deskripsinya terlihat lebih jelas dan tertata dan apabila file tersebut telah diedit (palsu) maka deskripsi file tersebut tidak jelas dan banyak sekali informasi yang mencurigakan.

DAFTAR PUSTAKA

AJI, 2013. Internet, Media Online, dan Demokrasi di Indonesia. Aliansi Jurnalis Independen Indonesia

ASLANIDOU, S. MENEXES, G. 2007. Youth and The Internet: Uses Practices in The Home. No.1375-1391. Vol. 51. ScienceDirect.

FARRUKH, A. etc. 2014. Youth Internet Safety: Risk, Responses and Research Recommendations. The Brookings Institution. Washington, DC.

- GASSER, U. etc. 2012. *Youth and Digital Media: From Credibility to Information Quality*. Harvard University. Cambridge USA.
- GAYED, T. etc. 2013. *Cyber Forensics: Representing and Managing Tangible Chain of Custody Using the Linked Data Principles*. ISBN: 978-1-61208-273-8. Iaria.
- JONES, L. etc. 2014. *A Content Analysis of Youth Internet Safety Programs: Are Effective Prevention Strategies Being Used?*. University of New Hampshire Research Center.
- LIVINGSTONE, S. 2011. *Internet, Children and Youth*. Oxford, UK.
- RALLINGS, J. 2015. *Youth and The Internet: a guide for policy makers*. Barnador's. Ilford UK.
- SHAH, A. RAVI, S. 2012. *A to Z of Cyber Crime*. Asian School of Cyber Laws. Mumbai, India.
- YULIANA, O. 2000. *Penggunaan Teknologi Internet dalam Bisnis*. No. 1. Vol. 2. Fakultas Ekonomi Universitas Kristen Petra.
- Databoks. 2018. *Katadata Indonesia*
- Undang-undang Republik Indonesia nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Jakarta: Kementerian Sekretariat Negara Republik Indonesia.