ANALISIS INVESTIGASI DAN PERANCANGAN KERANGKA KERJA FORENSIKA DIGITAL PADA MESIN FOTOKOPI *MULTI FUNCTION PERIPHERAL* (MFP)

TESIS

Diajukan Sebagai Salah Satu Syarat
Untuk Mendapatkan Gelar Pasca Sarjana
Magister Teknik Informatika

OLEH :

NAMA MHS. : MITRA UNIK
NO. INDUK MHS : 12 917 102
KONSENTRASI : FORENSIKA DIGITAL

MAGISTER TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS ISLAM INDONESIA

2015

LEMBAR PENGESAHAN DOSEN PEMBIMBING

ANALISIS INVESTIGASI DAN PERANCANGAN KERANGKA KERJA FORENSIKA DIGITAL PADA MESIN FOTOKOPI *MULTI FUNCTION PERIPHERAL* (MFP)

OLEH :

NAMA MHS. : MITRA UNIK
NO. INDUK MHS : 12 917 102

Yogyakarta, 6 Januari 2015

Pembimbing 1	Pembimbing 2
(Manik Hapsara, ST., M.Sc., Ph.D.,)	(Yudi Prayudi S.Si., M.Kom,)

Mengetahui
Direktur Program Pascasarjana
Fakultas Teknologi Industri
Universitas Islam Indonesia

(R. Teduh Dirgahayu, ST., M.Sc., Ph.D)

HALAMAN PENGESAHAN DOSEN PENGUJI

ANALISIS INVESTIGASI DAN PERANCANGAN KERANGKA KERJA FORENSIKA DIGITAL PADA MESIN FOTOKOPI *MULTI FUNCTION PERIPHERAL* (MFP)

TESIS

OLEH :

NAMA MHS. : MITRA UNIK

NO. INDUK MHS : 12 917 102

Telah Dipertahankan di Depan Sidang Penguji Sebagai Salah Satu Syarat
Untuk Mendapatkan Gelar Pasca Sarjana
Magister Teknik Informatika Fakultas
Teknologi Industri Universitas Islam Indonesia

Yogyakarta, 6 Januari 2015

Tim Penguji

Yudi Prayudi, S.Si.,M.Kom
Ketua

Ahmad Lutfi, S.Kom.,M.Kom
Anggota I

AKBP. Bakti Andriono, M.Kom
Anggota II

LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertanda tangan di bawah ini

Nama : Mitra Unik

NIM : 12 917 102

Tugas Akhir dengan judul :

ANALISIS INVESTIGASI DAN PERANCANGAN KERANGKA KERJA FORENSIKA DIGITAL PADA MESIN FOTOKOPI *MULTI FUNCTION PERIPHERAL* (MFP)

Menyatakan dengan sesungguhnya bahwa dalam tugas akhir ini tidak terdapat keseluruhan tulisan atau karya yang diambil dengan menyalin, meniru dalam bentuk rangkaian kalimat atau simbol atau algoritma atau program yang menunjukkan gagasan atau pendapat atau pemikiran orang lain, yang diakui seolah-olah sebagai tulisan atau karya sendiri.

Apabila di kemudian hari terbukti ada beberapa bagian dari karya ini adalah bukan hasil karya sendiri, tugas akhir yang diajukan sebagai hasil karya sendiri ini siap ditarik kembali dan siap menanggung risiko dan konsekuensi apapun.

Demikian surat pernyataan ini dibuat, semoga dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 6 Januari 2015

Yang Membuat Pernyataan

Mitra Unik

HALAMAN PERSEMBAHAN

Karya ini saya persembahkan kepada:

Ayahanda **Drs. Ahmad H.M Yusuf M.Pd** dan Ibunda **Evi yusnetti,**
yang senantiasa menjadi orang tua terhebat dan tak pernah menyerah
dalam usaha menghebatkan anak-anaknya.
Kedua saudara saya **Eko Hero** dan **Ratih Erissa** beserta keluarga,
yang selalu memberikan motivasi dan petuah-petuahnya.

Pada akhirnya saya persembahkan karya sederhana ini kepada semua pembaca,
untuk ditelusuri dan menjadi inspirasi yang bisa ditarik hikmahnya.

KATA PENGANTAR

Assalamualaikum Wr. Wb.

Alhamdulillah hirobbi 'alamin penulis ucapkan kepada ALLAH SWT yang selalu memberikan kesehatan dan keselamatan pada diri penulis untuk menyelesaikan tesis ini dengan judul "**ANALISIS INVESTIGASI DAN PERANCANGAN KERANGKA KERJA FORENSIKA DIGITAL PADA MESIN FOTOKOPI MULTI FUNCTION PERIPHERAL (MFP)"** sebagai persyaratan untuk mencapai gelar Magister Komputer pada program Pasca Sarjana Universitas Islam Indonesia.

Pada kesempatan ini dengan penuh kerendahan hati penulis haturkan ucapan terima kasih yang tak terhingga dan penghargaan yang setinggi-tingginya kepada Ayahanda **Drs. Ahmad H.M Yusuf M.Pd** dan Ibunda **Evi Yusnetti** serta Kakanda **Eko Hero** beserta istri (Siti Supiyah) dan Ayunda **Ratih Erissa Putri** beserta suami (Jufrizal Syachri) yang selalu memotivasi tiada henti memberi doa dan kasih sayangnya kepada penulis.

Di samping itu, secara khusus penulis haturkan terima kasih kepada:

1. Rektor UII Yogyakarta, Bapak Dr. Ir. Harsoyo, M.Sc dan para Pembantu Rektor.
2. Bapak Dekan Fakultas Teknologi Industri, Dr. Drs. Iman Djati Widodo, M.Eng., Sc. dan Ibu Wakil Dekan Dr. Sri Kusumadewi, S.Si., MT, atas motivasi, koreksi dan kemudahan pelayanan selama studi.
3. Bapak Direktur Program Pascasarjana, R. Teduh Dirgahayu, ST., M.Sc., Ph.D. dan para Asisten direktur atas segala fasilitas yang telah diberikan selama penulis menempuh studi.
4. Dosen pembimbing Bapak Manik Hapsara, ST., M.Sc., Ph.D., dan Yudi Prayudi, S.Si., M.Kom, Selaku dosen pembimbing, Terima kasih atas segala bantuan dukungan, semangat dan pengetahuannya serta kemudahan yang diberikan.

5. Dosen penguji progres, bapak Ahmad Lutfi, S.Kom.,M.Kom., dan AKBP Bakti Andriono, M.Kom., yang telah memberikan motivasi dan semangat serta bimbingan yang sangat berarti bagi penulis dalam menyelesaikan tesis ini.
6. Seluruh Dosen dan civitas Magister Teknik Informatika, baik secara langsung maupun tidak langsung telah membantu penulis selama masa-masa studi penulis.
7. Staf Administrasi dan tata usaha Magister Teknik Informatika,Universitas Islam Indonesia, yang telah membantu dalam segala urusan administrasi di kampus.
8. Rekan-rekan mahasiswa MTI angkatan 06 yang selama ini berjuang bersama dan selalu memberikan semangat satu sama lain.
9. Sahabat Mukti Rambe yang telah membantu penulis dalam melakukan penelitian dan memberikan tunjuk ajar.
10. Semua pihak yang telah membantu penulis selama penyusunan skripsi ini yang tidak dapat penulis sebutkan satu persatu.

Semoga Allah SWT senantiasa memberikan berkat dan anugrah-Nya berlimpah bagi beliau-beliau yang tersebut di atas. Sangat disadari dalam tesis ini terdapat banyak kekurangan oleh karena itu semua saran dan kritik penulis terima dengan lapang dada demi kesempurnaan penulisan tesis ini. Akhirnya harapan penulis semoga tesis ini bermanfaat bagi kita semua.

Wassalamu'alaikum Wr. Wb.

Yogyakarta, 6 Januari 2015

Mitra Unik

ABSTRAK

Kolaborasi teknologi komputer pada perangkat mesin fotokopi Multi-Function Peripheral (MFP) memicu meningkatnya produktivitas dan efisiensi terhadap entitas tersebut. Namun kolaborasi ini, juga melahirkan serangkaian praktek pelanggaran hukum. Belum adanya tool forensic analysis yang mampu melakukan investigasi secara static acquisition, memaksa seorang penyidik forensika digital harus mampu melakukan live acquisition di TKP pada barang bukti elektronik yang ditemukan. Padahal diketahui penanganan secara live acquisition merupakan penaganan yang mengandung risiko kehilangan barang bukti jika tidak dilakukan dengan prosedur dan regulasi yang jelas. Oleh sebab itu dibutuhkan penanganan khusus serta kerangka kerja khusus guna melakukan investigasi serta penggunaan teknik analisis yang sistematis sehingga mendapatkan artifak serta informasi mengenai kasus yang ditangani.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

Era digital dapat dicirikan sebagai terapan teknologi komputer sebagai alat yang meningkatkan cara-cara proses dari semulanya dikerjakan secara tradisional menjadi lebih modern. Kolaborasi teknologi/sistem komputer pada perangkat-perangkat pribadi, komersial, pendidikan, pemerintahan dan lainnya, memicu meningkatnya produktivitas dan efisiensi terhadap entitas tersebut. Integrasi teknologi komputer juga terjadi pada mesin fotokopi. Dimulai tahun 2002, mesin fotokopi analog bertransformasi menjadi mesin fotokopi digital atau disebut juga dengan mesin fotokopi *Multi Function Pheripheral* (MFP).

Multi Function Pheripheral (MFP) didefinisikan sebagai sebuah perangkat yang melakukan berbagai fungsi yang seharusnya dilakukan oleh perangkat satuan terpisah atau gabungan beberapa fungsi dalam satu perangkat (Rouse, 2011). Berbeda dengan mesin fotokopi analog, mesin fotokopi MFP tidak hanya saja berfungsi sebagai menyalin dokumen tulis (*copier*), namun juga telah dilengkapi dengan beberapa fitur seperti cetak (*printer*), pemindai (*scanning*), faksimile bahkan komunikasi *email* serta dilengkapi perangkat I/O yang dikonfigurasi dengan penyimpanan *non-volatile* (*hard drive*) sebagai lokasi penyimpan setiap rekaman berkas dari aksi dokumen yang dilakukan (CBSNews, 2010). Manfaat transformasi mesin fotokopi analog ke digital melahirkan kemudahan, kenyamanan, penghematan waktu, biaya dan tenaga dalam proses menyalin (Ifaorumhe, 2009).

Terlepas dari manfaatnya, mesin fotokopi memiliki ancaman tersendiri terkait hak cipta, misalkan saja bagi penerbit terhadap royalti dari hasil karya cipta, menurut Sommer 98% dokumen saat ini dihasilkan lewat bantuan peralatan digital. Sementara, di Amerika pada tahun 2008 diperkirakan terjadi kerugian sebesar US$ 66 Miliar akibat beberapa kasus yang disebabkan oleh kehilangan, pencurian,

pemalsuan dokumen-dokumen digital (Ademu, I. O., Imafidon, C. O., & Preston, 2011).

Regulasi terkait hak cipta telah diatur dalam Undang-Undang Hak Cipta Nomor 19 Tahun 2002. Hak Cipta merupakan hak eksklusif bagi Pencipta atau penerima hak untuk mengumumkan atau memperbanyak Ciptaannya atau memberikan izin untuk itu dengan tidak mengurangi pembatasan-pembatasan menurut peraturan per undang-undangan yang berlaku ("UU RI Nomor 19 Th 2002, Tentang Hak Cipta," 2002). Kasus pelanggaran hak cipta di Indonesia bukanlah merupakan hal yang baru, seperti yang diberitakan oleh surat kabar Online Tempo.co tertanggal Senin, 04 Agustus 2014 | 13:59 WIB, menyampaikan bahwa hasil operasi razia oleh Kepolisian Resort Kota Malang menetapkan seorang penjual buku di kompleks toko buku Jalan Wilis, Kota Malang, sebagai tersangka pembajakan buku. Pelaku dijadikan tersangka karena terbukti menjual buku bajakan terbitan PT. Salemba Empat Jakarta. Ditulis juga bahwa pelaku mengaku tidak mengetahui bahwa ratusan buku "setengah harga" tersebut merupakan buku bajakan yang ditawarkan oleh agen resmi sekitar dua bulan sebelum penangkapan pelaku (Bintariadi, 2007)

Bentuk-bentuk pelanggaran Hak Cipta atas buku dapat dikategorikan antara lain (Erlangga, 2013)

1. Hasil salin buku yang kemudian di perjual belikan
2. Pencetakan buku secara ilegal yang kemudian dijual dengan harga jauh di bawah buku asli
3. Penjualan *Electronic file* buku secara ilegal

UU No. 19 Tahun 2012 pasal 72 ayat 2 tentang Hak Cipta telah mengatur ketentuan pidana atas pelanggaran hak cipta atas buku, namun jika dilihat dari perspektif keilmuan forensika digital, pelanggaran hak cipta atas buku dapat dikategorikan ke dalam kejahatan teknologi komputer, yang ditafsirkan melalui penggunaan alat bantu ("UU RI Nomor 11 Tahun 2008, Tentang Informasi dan Transaksi Elektronik," 2008).

Forensika digital merupakan suatu disiplin ilmu yang mempelajari tentang penyelidikan kejahatan berbasis teknologi komputer. Penyelidikan forensika digital melibatkan penerapan serangkaian prosedur pada bukti digital seperti identifikasi, pelestarian, analisis dan pelaporan hasil. Selama proses analisis, peneliti forensika digital merekonstruksi peristiwa dengan memperhatikan artifak - artifak yang ditinggalkan guna mengevaluasi kebenaran dugaan-dugaan yang berkaitan dengan kejahatan atau insiden yang telah diidentifikasi dan diambil (Reith, Carr, & Gunsch, 2002).

Mesin fotokopi MFP sebagai barang bukti kejahatan komputer, tidak sepopuler perangkat lainnya seperti ponsel, komputer PC, leptop/*notebook, tablet*, *hard disk, flashdisk* dan perangkat penyimpanan *non-volatile* lainnya. Padahal mesin fotokopi MFP mampu menyimpan informasi serta rekam jejak penggunaan mesin fotokopi MFP (Willassen, 2014). Informasi-informasi tersebut bisa saja digunakan untuk menyelesaikan kasus pelanggaran dalam UU No. 19 Tahun 2012 pasal 72 ayat 2 tentang Hak Cipta. Ke tidak populeran ini, peneliti anggap cukup beralasan dikarenakan memang belum adanya pedoman dan serangkaian prosedur sistematis dalam proses penyelidikan perangkat mesin fotokopi MFP.

Prosedur dibutuhkan guna melindungi serta menjamin integritas barang bukti yang ditemukan, karena barang bukti digital bersifat mudah berubah, hilang atau rusak. Prosedur juga harus konsisten dan terdefinisi baik dengan kebijakan umum penyelidikan yang dapat menjelaskan tahapan penerimaan, proses akuisisi, pemeriksaan, analisis dan dokumentasi dari penanganan bukti serta produk yang terkait dengan penyelidikan. Jika penanganan barang bukti tersebut tidak prosedural dan oleh orang yang tidak memiliki tingkat kompetensi yang cukup di bidang forensika digital, maka akan sangat mungkin bukti digital sebelumnya rusak, berubah bahkan hilang sehingga barang bukti tersebut tidak dapat membuat terang kasus kejahatan tersebut.

Maka dari itu tesis ini akan menyajikan hasil pemeriksaan forensika digital, yang berfokus pada penelitian forensika digital mesin fotokopi MFP serta perancangan prosedur penyelidikan yang sistematis dan efisien. Pemeriksaan

forensika digital pada perangkat MFP ini, akan penulis lakukan pada mesin fotokopi merek Canon seri iR 6000 karena mesin fotokopi tersebut dianggap merupakan mesin fotokopi yang paling banyak dan populer digunakan untuk kebutuhan usaha komersial di Indonesia (Fotocopy Global, 2013)

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang di atas dirumuskan yang menjadi pokok permasalahan adalah:

1. Bagaimanakah teknik akuisisi forensika digital secara langsung (*Live Acquisition*) maupun tidak (*Static Acquisition*) pada perangkat mesin fotokopi *Multi Function Peripherals* (MFP)?
2. Artifak-artifak apa saja yang dapat ditemukan pada perangkat mesin fotokopi *Multi Function Peripherals* (MFP)?
3. Bagaimanakah teknik akuisisi yang paling ideal pada pada mesin fotokopi *Multi Function Peripherals* (MFP)?
4. Bagaimana rancangan Skema kerja akuisisi forensika digital pada mesin fotokopi *Multi Function Peripherals* (MFP)*?*

1.3 Batasan Masalah

Rumusan masalah di atas dibatasi dengan beberapa hal sebagai berikut:

1. Objek penelitian pada tugas akhir ini adalah perangkat mesin fotokopi *Multi Function Peripherals* (MFP).
2. Mesin fotokopi yang digunakan pada penelitian ini adalah mesin fotokopi jenis *Multi Function Peripherals* (MFP) merk Cannon iR6000.
3. Perancangan Kerangka kerja penyelidikan digital mesin fotokopi diperuntukkan bagi fotokopi jenis *Multi Function Peripherals* (MFP).

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah:

1. Mengetahui teknik akuisisi forensika digital secara langsung (*Live Acquisition*) maupun tidak (*Static Acquisition*) pada perangkat mesin fotokopi *Multi Function Peripherals* (MFP).
2. Mengetahui artifak-artifak digital yang terdapat pada mesin fotokopi *Multi Function Peripherals* (MFP).
3. Mengetahui teknik akuisisi yang ideal pada penyelidikan forensika digital perangkat mesin fotokopi *Multi Function Peripherals* (MFP).
4. Merancang Kerangka penyelidikan forensika digital mesin fotokopi *Multi Function Peripherals* (MFP).

1.5 Manfaat Penelitian

Hasil penelitian ini diharapkan dapat memberikan:

1. Secara teoritis, memberikan manfaat terhadap pengembangan ilmu Forensika Digital
2. Secara praktis, menjadi bahan masukan kepada ahli forensika digital ketika melakukan proses investigasi mesin fotokopi pada umumnya.

1.6 Metodologi Penelitian

1.6.1 Studi Pendahuluan

Studi Pendahuluan dilakukan untuk mempertajam arah studi utama. Menurut Prof. Dr. Winarno Surachmad, studi pendahuluan disebut sebagai *Exploratory*, yaitu sebagai kemungkinan diteruskannya pekerjaan meneliti dan mencari informasi yang diperlukan oleh peneliti agar masalah menjadi lebih jelas kedudukannya (Eka Surya, 2014). Studi pendahuluan meliputi studi literatur dan pengumpulan data. Seperti teori pengumpulan data pada umumnya, maka sumber-sumber pengumpulan informasi untuk mengadakan studi pendahuluan ini didapatkan dari 3 (tiga) sumber informasi utama.

1. *Paper* (Studi Literatur): Meliputi dokumen, buku, majalah atau bahan tertulis lainnya, baik berupa teori, laporan penelitian atau penemuan sebelumnya baik bersifat *Online source* maupun *Offline source.*
2. *Person*: Dilakukan dengan cara bertemu, bertanya dan berkonsultasi dengan para ahli.
3. *Place:* Berupa tempat, lokasi atau benda-benda yang terdapat di tempat penelitian.

1.6.2 Pengembangan Pengumpulan Data

Penelitian akan memperoleh tujuan yang diharapkan apabila didukung oleh data yang valid (*sahih*) dan reliabel. Untuk memperoleh data yang valid dan reliabel diperlukan teknik tertentu sebagai alat pengumpul data di dalam penelitian. Terdapat tahapan umum dalam mengembangkan atau menyusun teknik pengumpul data pada penelitian ini, yaitu pengamatan objek penelitian, pemodelan komputer forensik, perancangan pemodelan dan implementasi.

1.6.3 Analisis dan Implementasi

Analisis dan implementasi, dinyatakan dengan pembuatan laporan penelitian dari level perencanaan, perancangan hingga proses implementasi penelitian dengan asumsi penelitian telah selesai dilakukan.

1.7 Review Literatur

Terdapat dua jenis pendekatan secara umum pada forensika digital yaitu keilmuan komputer dan penyelidikan. Tujuan umum dari setiap proses penyelidikan forensik adalah pembuktian, yaitu upaya menemukan potongan diskrit informasi. Pendekatan ilmu komputer forensik digital dapat dijumpai dari karakteristik data yang digunakan atau yang menyertai data tersebut seperti Metadata. Sedangkan pendekatan penyelidikan digunakan sebagai pemeriksaan bukti-bukti untuk menafsirkan data ke dalam keterangan fakta yang diketahui dan unsur-unsur kejahatan dalam rangka untuk menentukan informasi pembuktian (Pollitt, 2009).

Berbagai teknik ditawarkan dari cerminan dua buah pendekatan tersebut, khususnya yang berkaitan dengan penyelidikan forensik mesin fotokopi. Penyelidikan tidak hanya dilakukan untuk memeriksa hasil (dokumen cetak) saja, namun juga meliputi penyelidikan perangkat mesin itu sendiri. Seperti sebuah penelitian yang dilakukan oleh Sein Yngvar Willasen, M.Sc, seorang manager penyelidikan komputer forensik di Ibas AS. Willasen mengutarakan tingginya dukungan penggunaan mesin fotokopi pada aktivitas bisnis yang masih mengandalkan dokumen cetak guna operasional sehari-hari. Mesin fotokopi yang dilengkapi dengan *hard drive*, pada prinsipnya tetap dapat menyimpan informasi walau saat *shut down.* Uji coba yang dilakukan untuk mengambil kemungkinan salinan dokumen yang terdapat pada saat sebelum/setelah dokumen dicetak atau disalin pada mesin fotokopi. Untuk membuktikan kemungkinan tersebut Willassen melakukan analisis menggunakan Encase 3.20 pada dua buah mesin fotokopi digital Xerox DC432ST dan iR2200. Hasilnya, didapat 4 (empat) buah partisi yang tidak satu pun memiliki *readable system* pada Encase. Kesimpulan yang disampaikan Willassen dalam makalahnya, bahwa mungkin untuk mengambil dokumen-dokumen dengan melakukan analisis forensik *hard drive* yang dapat ditemukan pada sebagian besar mesin fotokopi modern. (Willassen, 2014).

Sistem penyimpanan data citra pada *hard disk* di perangkat mesin fotokopi MFP juga di bahas secara detail dalam sebuah publikasi paten. *Patent Application Publication* tersebut, di katakan sebuah perangkat penyimpanan data citra pada mesin fotokopi MFP meliputi unit masukan data citra, unit perekaman data citra, unit pengolahan kompresi, unit keputusan lokasi, dan unit kontrol kompresi. Unit input data citra menerima masukan dari data citra. Unit perekaman data *image*, merekam masukan data citra dari unit masukan data citra. Unit pengolahan kompresi data citra akan dicatat ke dalam unit rekaman data citra. Unit penentuan lokasi memutuskan apakah atau tidaknya data citra yang telah dimasukkan oleh unit masukan data citra adalah data citra yang berkaitan dengan bagian lokasi dari suatu citra. Serta data unit kontrol kompresi mengontrol unit pengolahan kompresi sehingga kompresi pengolahan dapat dibatalkan untuk data citra yang telah di tentukan berdasarkan unit penentuan lokasi menjadi data citra yang terkait. Dari

paten ini dapat diasumsikan bahwa media penyimpanan *non-volatile* digunakan sebagai inti dari pemrosesan kerja mesin fotokopi MFP (Mizuyama, 2007).

Pada ranah yang berbeda penyelidikan forensika digital mesin fotokopi dapat dilakukan dengan pendekatan penyelidikan forensika kimia, yaitu dengan memperhatikan hasil cetakan pada mesin fotokopi. Penelitian oleh Rena A. Merrill, dkk, dilakukan dengan meneliti perbedaan hasil cetak antara printer dan mesin fotokopi melalui pengujian penggunaan tinta cetak. Penelitian dilakukan dengan memfokuskan *microscopically reflection-absorption by infrared spectroscopy (R-A IR)* dianggap sebagai teknik yang layak untuk menganalisis resin polimer kering yang terkandung di dalam tinta printer dan salinan oleh fotokopi. Teknik pengambilan sampel melibatkan perpindahan panas dari tinta dokumen ke permukaan reflektif aluminium foil diikuti dengan analisis oleh R -A IR. Selain itu Rena A. Merrill dkk, beranggapan teknik ini merupakan teknik yang sederhana, cepat dan tersedia untuk sebagian besar laboratorium forensik (Merrill, Bartick, & Taylor, 2003).

Mengenai penyusunan prosedur forensika digital serta bukti digital (Al-azhar, 2012) mengemukakan, penanganan penyelidikan forensika digital oleh ahli forensika digital mesti menerapkan pelaksanaan kegiatan secara prosedural. Prosedural tersebut dikenal dengan istilah *triage forensik.* *Triage forensik* ditujukan untuk menyelamatkan objek investigasi berupa perlakuan pada barang bukti digital. *Triage forensik* juga memiliki tujuan untuk mendapatkan data-data digital secara cepat dari barang bukti elektronik. Ini dimaksudkan agar investigator dapat menentukan langkah investigasi lanjutan dengan benar dan secara cepat dapat melacak keberadaan pelaku dan menangkapnya. Tanpa prosedur yang jelas dan terdefinisi dengan baik proses forensika digital dapat memakan waktu yang lama dan berimbas pada kecepatan investigasi yang menjadi lambat untuk menentukan tahapan penyelidikan selanjutnya, atau bahkan memberikan peluang bagi pelaku untuk menghilangkan jejak kejahatannya.

1.8 Sistematika Penulisan

Sistematika penulisan merupakan daftar susunan bab dan subbab dari sebuah karya tulis. Laporan penelitian ini disusun dalam sistematika dan berstruktur agar lebih mudah dipahami bagi siapa saja yang membacanya. Sistematika laporan penelitian ini adalah sebagai berikut.

BAB I PENDAHULUAN

Bab ini memuat latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian yang digunakan dalam penelitian serta sistematika penelitian.

BAB II LANDASAN TEORI

Bab ini memuat teori-teori penunjang yang digunakan sebagai dasar penelitian penyelidikan forensika digital terhadap mesin fotokopi MFP.

BAB III METODOLOGI

Uraian dalam bab ini merupakan penjabaran lebih rinci tentang metode penelitian yang secara garis besar telah disajikan di Bab I (Pendahuluan).

BAB IV HASIL DAN PEMBAHASAN

Bagian ini pada dasarnya memuat pengolahan dan analisis data untuk menghasilkan temuan dan pembahasan /analisis dari hasil temuan. Pengolahan data dilakukan berdasarkan prosedur penelitian yang telah diurai di Bab III.

BAB V KESIMPULAN DAN SARAN

Dalam Bab V disajikan penafsiran dan pemaknaan peneliti terhadap hasil analisis temuan penelitian, yang disajikan dalam bentuk kesimpulan penelitian. Serta di kemukakan beberapa saran untuk dilaksanakan guna pengembangan lebih lanjut terkait tugas akhir ini.

BAB II

LANDASAN TEORI

2.1 Forensika Digital

Forensika digital merupakan aplikasi ilmu pengetahuan dan teknologi komputer untuk melakukan pemeriksaan dan analisis terhadap barang bukti elektronik dan barang bukti digital dalam melihat keterkaitannya dengan kejahatan (Al-azhar, 2012). Forensika digital merupakan pendekatan dari keilmuan komputer dan penyelidikan, tujuan dari dua buah pendekatan tersebut yaitu menemukan potongan artifak informasi sebagai pembuktian. Dalam keilmuan komputer, karakteristik data atau meta data merupakan hal yang diperhatikan sedangkan pendekatan penyelidikan mengulas isi bukti untuk menafsirkan data untuk mendapatkan fakta dalam unsur-unsur kejahatan dalam rangka menemukan informasi pembuktian atau informasi dari barang bukti (Pollitt, 2009).

Pollitt memberikan salah satu definisi awal dari forensik digital,

> *"[Digital] forensics is the application of science and engineering to the legal problem of digital evidence. It is a synthesis of science and law. At one extreme is the pure science of ones and zeros. At this level, the laws of physics and mathematics rule. At the other extreme, is the courtroom."* (Pollitt, 1995a)

McKemmish menjelaskan forensik digital dengan cara sebagai berikut Forensik Digital adalah:

> *"The use of scientifically derived and proven methods for the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations."* (McKemmish, 1999).

McKemmish menunjukkan bahwa forensik digital merupakan domain multidisiplin. Palmer mendefinisikan Forensika Digital sebagai:

> *"The use of scientifically derived and proven methods for the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations."* (Palmer, 2001)

Forensika digital merupakan bidang spesialisasi komputer untuk kepentingan pembuktian hukum (*Pro Justice*) dari kejahatan komputer (*computer crime*), sebagai upaya menjerat pelaku kejahatan. penggunaan ilmu dan metode forensika digital ditujukan untuk menemukan, mengumpulkan, mengamankan, menganalisis, menginterpretasi dan mempresentasikan barang bukti digital yang terkait dengan kasus yang terjadi untuk kepentingan rekonstruksi kejadian serta keabsahan proses keadilan (Agarwal & Gupta, 2011). Oleh karena itu, ada ketergantungan pada daerah non-teknis, terutama mengingat fondasi dari forensika digital merupakan multidisiplin keilmuan (komputasi dan hukum) (Yasinsac, Erbacher, Marks, Pollitt, & Sommer, 2003).

Mendapatkan pengakuan dari pengadilan setidaknya membutuhkan dua hal. Pertama, informasi harus faktual. Kedua, harus diperkenalkan oleh ahli yang dapat menjelaskan fakta-fakta dan menjawab pertanyaan. Hal pertama menyangkut keilmuan dan yang kedua membutuhkan pengalaman, pelatihan dan kemampuan untuk mengkomunikasikan ilmu pengetahuan tersebut (Pollitt, 1995a). Selain itu M.Pollitt memperluas konsep ini dengan mengatakan:

> *"Investigators and others have, by trial and error, evolved methods which will allow the discovery of evidence form storage media that will satisfy the twin requirements of science and law"* (Pollitt, 1995b).

Dapat dipahami bahwa tujuan akhir dari forensika digital adalah untuk memberikan bukti digital yang sah dan benar di pengadilan, serta tidak hanya sekedar memeriksa peralatan digital atau menganalisis data digital. Hal ini ditegaskan agar forensika digital dapat dipahami bukan sebatas subjek yang hanya

berisi masalah teknis, namun merupakan disiplin yang berhubungan dengan keilmuan komputer dan permasalahan hukum. Singkatnya, forensika digital adalah suatu rangkaian metodologi yang terdiri dari teknik dan prosedur untuk mengumpulkan bukti-bukti berbasis entitas maupun peranti digital agar dapat dipergunakan secara sah sebagai alat bukti di pengadilan (Eko Indrajit, 2014).

2.1.1 Metodologi dan Prosedur Umum Forensika Digital

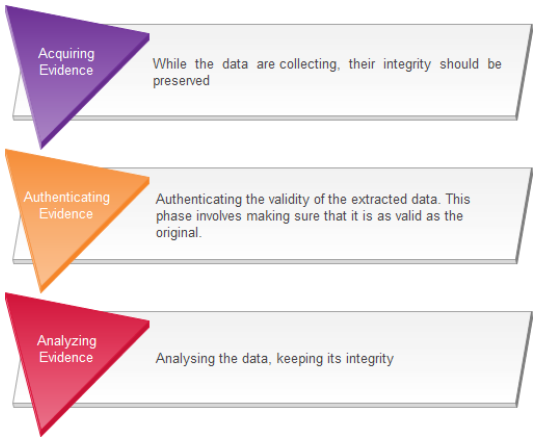
Proses hukum dalam penyelidikan komputer yang berpotensi melakukan tindak pelanggaran, sangat tergantung pada standar per undang-undangan dan peraturan yang berlaku pada daerah setempat. Keaslian dan integritas bukti merupakan hal yang sangat penting. Langkah pertama adalah membentuk mata rantai kebijakan organisasi, seperti setiap bagian dari bukti yang dikumpulkan bertanggung jawab pada seorang individu hingga dikembalikan ke pemiliknya (Reith et al., 2002).

ACPO (*Association of Chief Police Officers*) membuat panduan pemeriksaan barang bukti digital. Terdapat empat prinsip utama pada penanganan barang bukti digital (ACPO, 2012):

1. Prinsip 1: Tidak ada tindakan yang diambil oleh badan-badan penegak hukum atau agen mereka yang mengubah data yang ada pada sebuah komputer atau media penyimpan yang kemudian dapat dijadikan bukti di pengadilan.
2. Prinsip 2: Dalam keadaan luar biasa, di mana seseorang dirasa perlu untuk mengakses data asli yang ada pada komputer atau pada media penyimpanan, orang tersebut adalah orang yang benar-benar kompeten untuk melakukannya dan mampu memberikan bukti, menjelaskan relevansi dan implikasi dari tindakannya.
3. Prinsip 3: *Audit trail* atau catatan lain dari semua proses yang diterapkan untuk komputer berbasis bukti elektronik harus diciptakan dan dipelihara. Pihak ketiga yang independen harus mampu memeriksa proses-proses dan mencapai hasil yang sama.

4. Prinsip 4: Orang yang bertanggung jawab atas penyelidikan (petugas kasus) memiliki tanggung jawab keseluruhan untuk memastikan bahwa hukum dan prinsip-prinsip ini dipatuhi.

Prosedur penanganan barang bukti merupakan isu penting di bidang forensika digital. Kualitas, validitas dan kredibilitas bukti digital sangat dipengaruhi oleh prosedur penanganan yang diterapkan untuk mendapatkan dan menganalisa bukti. Prosedur forensika digital dijalankan untuk memastikan integritas bukti yang dikumpulkan dari barang bukti elektronik. Prosedur forensika digital melibatkan pelestarian, identifikasi, ekstraksi, dokumentasi dan interpretasi data komputer (Kruse, & Heise, 2001). Menurut Kruse dan Heise pendekatan metodologi berbasis pada tiga komponen utama.



Gambar 2. 1 Model Kruse dan Heise 2001

Menurut DFRWS (*Digital Forensik Research Works Shop*) proses penyelidikan forensika digital memiliki 7 (Tujuh) tahapan yang masing-masing proses memiliki tahapan kebutuhan dan pencarian, yaitu *"Identification, preservation, Colection, examination, analysis, presentation, and decision ".*

Reith dan rekan menekankan manfaat dari prosedur umum dari forensika digital yaitu memungkinkan untuk sebuah metodologi yang konsisten dari masa lalu, sekarang dan masa depan dalam rangka penyelidikan perangkat digital yang dapat diterima dan dipahami secara luas baik perangkat tersebut sudah atau belum

direalisasikan (Reith et al., 2002). Reith dan rekan juga mengidentifikasi minimnya penerapan *Standar Operational Procedure* (SOP) saat penyelidikan lapangan dikarenakan keunikan kasus dan perubahan teknologi serta undang-undang yang berbeda. Oleh sebab itu, penggunaan SOP yang fleksibel yang tidak terbatas pada satu jenis proses dan sistem, menjadi solusi untuk mengatasi permasalahan tersebut.

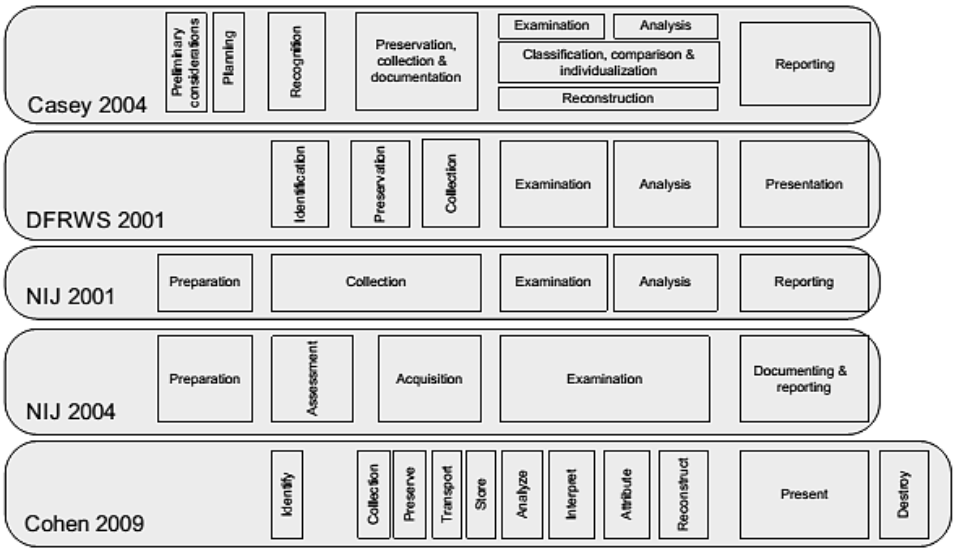
Reith dan rekan, juga mengajukan model pengolahan yang disebut dengan *Abstract Digital Forensics Model* (ADFM). ADFM memiliki sembilan tahapan kunci penyelidikan forensika digital (Reith et al., 2002).

1. Identifikasi (*Identification*): Mengidentifikasi dan menentukan jenis kejadian.
2. Persiapan (*Preparation*): Surat perintah penggeledahan, mengatur alat yang diperlukan, dan teknik yang dibutuhkan.
3. Strategi pendekatan (*Approach Strategy*): Membangun sebuah pendekatan yang dinamis untuk memaksimalkan pengumpulan barang bukti dan meminimalkan dampak pada korban.
4. Pelestarian (*Preservation*): Melindungi dan menjaga barang bukti.
5. Pengumpulan (*Collection*): Mencatat seluruh informasi terkait bukti elektronik serta mengambil gambar dengan prosedur yang tepat.
6. Pemeriksaan (*Examination*): Lakukan pencarian yang teliti dan terperinci guna mendapatkan bukti yang relevan dengan kejadian.
7. Analisis (*Analysis*): Memberikan interpretasi bukti untuk membangun hipotesis penyelidikan dan menawarkan kesimpulan berdasarkan bukti.
8. Presentasi (*Presentation*): Memberikan penjelasan kesimpulan.
9. Mengembalikan bukti (*Returning Evidence*): Memastikan bahwa aset fisik dan digital dikembalikan kepada pemilik.

Tujuan penyelidikan adalah untuk mengungkap dan menyajikan kebenaran. Kesalahan dalam penyelidikan, khususnya di ranah forensika digital akan membawa dampak yang buruk bagi proses peradilan dalam mencari kebenaran. Kebenaran penyelidikan bergantung pada usaha untuk menggunakan metodologi tepercaya dan teknik untuk memastikan bahwa analisis, interpretasi,

dan pelaporan yang objektif dan transparan. Walau pada dasarnya metode penyelidikan digital bervariasi menurut faktor teknis seperti jenis komputasi atau perangkat komunikasi, apakah penyelidikan adalah dalam kasus pidana, perdata, komersial, militer atau konteks lainnya, namun jika diamati secara mendalam setiap metodologi memiliki kesamaan pada perspektif proses, prinsip dan metode (Casey & Schatz, 2011).

Urutan kegiatan, identifikasi, pelestarian, analisis, dan presentasi, bisa dikatakan adalah dasar dari model proses pandangan investigasi digital.



Gambar 2. 2 Perbandingan terminologi yang berhubungan dengan model proses investigasi digital (Casey & Schatz, 2011)

Smith Petreski mengambil kesimpulan terhadap pentingnya metodologi forensika digital:

1. Tahapan jelas dan lebih baik dari informasi par analisis
2. Mencapai estimasi yang lebih baik dari investigasi yang diperlukan
3. Optimalkan waktu untuk mencapai tujuan kasus
4. Memberikan hasil yang lebih konsisten dari tim penyelidik forensik digital
5. Menyediakan Kerangka kerja untuk memprediksi analisis waktu, sumber daya, dan biaya

2.1.2 Aturan Forensika Digital

Hasil akhir dari forensika digital pada hakikatnya tunduk pada pengawasan yudisial. Metodologi yang digunakan dalam proses forensika digital harus dipilih agar tidak membahayakan aturan yang relevan. Aturan forensika digital adalah (McKemmish, 1999) :

1. Minimalisir penanganan menggunakan barang bukti asli

   Setiap pemeriksaan bukti asli harus dilakukan sedemikian rupa agar meminimalkan kemungkinan alterasi. Bila memungkinkan penanganan ini dapat dilakukan dengan menduplikasi barang bukti asli dan pemeriksaan dilakukan pada barang bukti hasil duplikasi.
2. Menghitung setiap perubahan

   Setiap perubahan pada barang bukti harus di dokumentasi. Hal ini berlaku pada fisik dan pada tingkat *logic*. Pemeriksa harus mampu mengidentifikasi dengan benar tingkat apapun berubah dan memberikan penjelasan rinci tentang mengapa perubahan itu perlu.
3. Memenuhi aturan dari barang bukti

   Penggunaan aplikasi, *tool* forensik dan teknik forensik harus relevan dengan barang bukti yang akan di akuisisi. Salah satu dasar ajaran kebutuhan komputasi forensik adalah untuk memastikan bahwa penerapan alat dan teknik tidak mengurangi integritas dari hasil akhir pemeriksaan barang bukti
4. Jangan melakukan di luar pengetahuan anda

   Ahli forensika digital tidak harus melakukan pemeriksaan di luar tingkat pengetahuan mereka. Penting, bahwa ahli forensik dapat menggambarkan secara benar proses yang digunakan selama pemeriksaan dan menjelaskan metodologi yang mendasari untuk proses tersebut.

2.1.3 Fokus Forensika Digital

Aktivitas forensika digital dilakukan dalam dua konteks utama. Pertama adalah konteks terkait dengan pengumpulan dan penyimpanan data berisi seluruh rekaman detail mengenai aktivitas rutin yang dilaksanakan oleh organisasi atau perusahaan tertentu yang melibatkan teknologi informasi dan komunikasi. Dan kedua adalah pengumpulan data yang ditujukan khusus dalam konteks adanya suatu tindakan kejahatan berbasis teknologi.

Fokus yang dikumpulkan dapat dikategorikan menjadi tiga domain utama, yaitu (Eko Indrajit, 2014):

1. *Active data*

   Merupakan informasi terbuka dapat dilihat oleh siapa saja, terutama data, program maupun file yang dikendalikan oleh sistem operasi.
2. *Archival Data*

   Merupakan informasi yang telah menjadi arsip sehingga telah disimpan sebagai backup dalam berbagai bentuk alat penyimpan seperti hardisk eksternal, CD ROM, **B**ack Up tape, DVD, dan lain-lain.
3. *Latent Data*

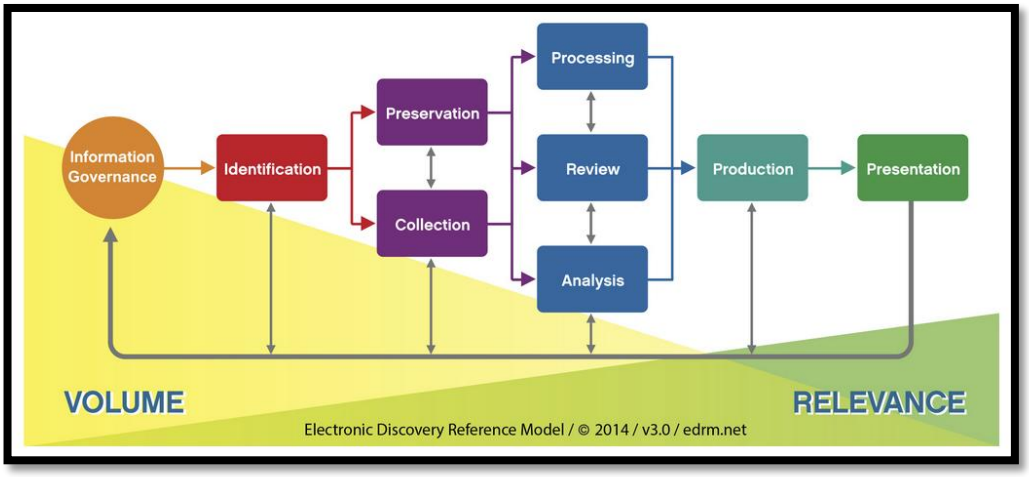
   Merupakan informasi yang membutuhkan alat khusus untuk mendapatkannya karena sifatnya yang khusus, misalnya: telah dihapus, ditimpa data lain, rusak (*corrupted file*), dan lain sebagainya.

2.2 *Electronic Discovery Reference Model* (EDRM)

EDRM merupakan relativitas baru yang banyak digunakan di dalam aktivitas akuisisi bukti elektronik. EDRM menggambarkan pandangan secara konseptual dari proses penemuan barang bukti elektronik serta proses berulang-ulang yang dimaksudkan sebagai dasar guna mengakuisisi serta menganalisis barang bukti elektronik pada aktivitas investigasi forensika digital (Edrm.net, 2005).

Electronic Discovery (atau Digital Investigasi Forensik) didefinisikan sebagai proses identifikasi, melestarikan, menganalisis dan menyajikan bukti

digital dengan cara yang diterima secara hukum (McKemmish, 1999). Empat tahap utama tersebut juga ditemukan di EDRM.



Gambar 2. 3 Electronic Discovery Reference Model (EDRM) (Edrm.net, 2005).

Meninjau definisi yang di rumuskan oleh McKemmis tersebut, dapat di golongkan menjadi empat perbedaan utama dari tahapan tersebut.

1. Identifikasi dilakukan guna mengetahui bukti apa saja yang hadir, di mana dan bagaimana bukti tersebut disimpan. Langkah ini mesti dilalui agar seorang ahli forensika digital dapat mengetahui langkah penyelidikan yang ditempuh dan menggunakan alat yang tepat untuk mengakuisisi. Komputasi forensik bukanlah semata-mata hal yang dijadikan fokus utama, korelasi dengan perangkat elektronik yang mampu sebagai tempat penyimpanan informasi seperti ponsel, buku harian elektronik dan *smart card* mesti juga ditindak lanjuti.
2. Pelestarian bukti digital adalah elemen penting pada proses forensik. Setiap pemeriksaan elektronik berpotensi mengubah data maupun meta data sehingga nilai integritas di mata hukum menjadi hilang. Perubahan data yang tidak dapat dihindari, penjelasan formal dan terperinci mestilah dilakukan seperti sifat serta alasan mengapa perubahan data tersebut

terjadi. Pencatatan perubahan tersebut tidak hanya terbatas pada data itu sendiri, namun juga pada perubahan fisik.

3. Analisis bukti digital, pengolahan dan interpretasi data digital dianggap sebagai unsur utama dari forensik komputasi. Setelah di ekstrak bukti digital membutuhkan pengolahan sebelum dapat dibaca orang awam. Sebagai contoh ketika isi *hard disk* di *imaging* (dicitrakan), data yang tersimpan di dalam citra masih membutuhkan proses sehingga data dapat di ekstrak guna dipahami sebagai bahasa yang dapat dimengerti orang awam (manusia).
4. Menyajikan bukti digital melibatkan bukti saat presentasi di pengadilan hukum, termasuk teknik presentasi, keahlian dan kualifikasi ahli serta kredibilitas proses yang digunakan untuk bukti yang di hadirkan. Keterangan ahli ialah apa yang seorang ahli nyatakan di sidang pengadilan ((“Kitab Undang-Undang Hukum Acara Pidana (KUHAP) Undang-Undang Nomor 8 Tahun 1981,” 1981) Pasal 186).

Beberapa istilah yang digunakan dalam definisi McKemmish juga digunakan dalam EDRM. Seluruh proses, setiap langkah dan setiap keputusan pemeriksaan forensik membutuhkan dokumentasikan. Setelah setiap tahap, dan dalam beberapa kasus bahkan setelah tugas masing-masing, validasi perlu dilakukan oleh pemeriksa lain. Hal ini memastikan bahwa proses telah dilakukan tanpa cacat.

2.3 Barang Bukti Forensika Digital

Pentingnya peningkatan dalam investigasi serta penggunaan barang bukti di pengadilan, ahli forensik mesti memiliki pemahaman dasar dari definisi bukti digital dan potensi sumber barang bukti. *Digital evidence* atau dalam bahasa Indonesia yaitu bukti digital atau bukti elektronik adalah setiap informasi pembuktian disimpan atau ditransmisikan dalam bentuk digital yang pihak untuk kasus pengadilan dapat menggunakan di pengadilan. (Eoghan, 2004)

Menurut Andriono barang bukti memiliki nilai sakral di mana seorang investigator dan *forensik analyst* dapat mengungkap kasus-kasus tersebut dengan

kronologis yang lengkap, untuk kemudian melacak keberadaan pelaku dan menangkapnya (Andriono, 2013). Selanjutnya, Andriono mengklasifikasikan barang bukti forensika digital menjadi:

1. Barang bukti elektronik. Barang bukti ini bersifat fisik dan dapat dikenali secara visual, oleh karena itu, investigator dan ahli forensika digital harus sudah memahami untuk kemudian dapat mengenali masing-masing barang bukti elektronik ini ketika sedang melakukan proses *searching* (pencarian) barang bukti di TKP. Jenis-jenis barang bukti elektronik adalah sebagai berikut :
    a. Komputer PC, laptop/*notebook, netbook, tablet*
    b. *Handphone, smartphone*
    c. *Flash disk/thumb drive*
    d. *Floppy disk*
    e. *Hard disk*
    f. CD/DVD
    g. *Router, switch, hub*
    h. Kamera video, CCTV
    i. Kamera digital
    j. *Digital recorder*
    k. *Music*/*video player*
2. Barang bukti digital. Barang bukti digital barang bukti ini bersifat digital yang di ekstrak atau di-*recover* dari barang bukti elektronik. Barang bukti ini di dalam Undang-Undang No. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik dikenal dengan istilah informasi elektronik dan dokumen elektronik.

Sejumlah barang bukti elektronik menyimpan artifak-artifak yang selanjutnya disebut dengan bukti digital. Artifak didefinisikan sebagai *Information or data created as a result of the use of an electronic device that shows past activity.* Menurut *Scientific Working Groups on Digital Evidence and Imaging Technology*, bukti digital yang juga dikenal dengan sebutan *electronic evidence* atau *digital*

evidence didefinisikan sebagai *information of probative value that is stored or transmitted in digital form.*

Definisi lain yang senada, bukti digital adalah informasi dan data nilai penyelidikan yang disimpan, diterima atau dikirim dari perangkat elektronik (DeGaine, Jacqueline J, & Major, 2014). Bukti digital dapat ditemukan pada sejumlah perangkat elektronik. Bukti digital bisa berupa bukti riil maupun abstrak (perlu diolah kembali sebelum menjadi bukti yang riil).

Dalam sistem hukum Indonesia pada saat ini, Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik memang tidak secara langsung memberikan definisi atas apa yang dimaksud dengan bukti elektronik. Namun, bila melihat ketentuan yang terdapat dalam Undang-Undang tersebut maka dapat disimpulkan, bahwa yang dimaksud dengan bukti elektronik adalah informasi elektronik dan/atau dokumen elektronik, yaitu satu atau sekumpulan data elektronik, yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan Dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan, dan/atau didengar melalui Komputer atau Sistem Elektronik termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic Mail*), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

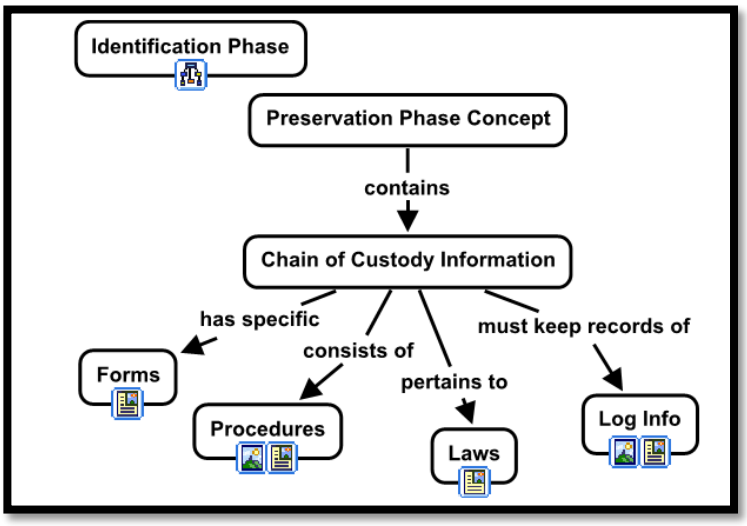
Barang bukti digital memiliki dua jenis sifat penyimpanan, *non-volatile* dan *volatile*. *Non-volatile* mengandung pengertian penyimpanan memori komputer tidak hilang bila daya dimatikan. Data yang tersimpan pada magnetik (disk, disket, tape) atau magnetik optik (CD, DVD) media dan dalam beberapa perangkat semikonduktor (silikon), sedangkan *volatile* adalah penyimpanan memori/informasi yang disimpan pada *random access memory* (RAM) dan hilang jika daya diputuskan (Businessdictionary, 2014).

2.4 Manajemen Barang Bukti

Merujuk beberapa definisi pada subbab sebelumnya, forensika digital merupakan analisa forensik dari sistem komputer melibatkan pengumpulan, identifikasi benda yang mencurigakan atau peristiwa dan kemudian dilakukan penyelidikan yang mendalam atau detail guna membentuk hipotesis mengenai sebab akibat suatu permasalahan sehingga dapat disajikan di pengadilan. Ahli forensika digital harus mampu menjaga integritas bukti tersebut. Adanya dua istilah dalam manajemen barang bukti antara lain *the chain of custody* dan *rules of evidence.*

2.4.1 *The Chain of Custody*

Satu hal terpenting yang harus dilakukan investigator adalah untuk melindungi bukti. *Chain of Custody* berhubungan dengan pelestarian barang bukti. Dokumentasi menyeluruh dari rantai pemeriksaan memberikan rincian lengkap tentang kepemilikan dan lokasi bukti selama masa kasus. Rincian tersebut untuk menghindari tidak diakuinya integritas barang bukti di pengadilan (Tanner & Dampier, 2009). Tanner dan Damper menambahkan, *Chain of custody* menetapkan bukti yang dikumpulkan ("*Form*" *concept*), bagaimana dan di mana bukti tersebut dikumpulkan (*"Forms"* dan *"Procedures" concepts*), yang mengambil alih bukti (*"Log Info" concept*), bagaimana bukti tersebut dilindungi dan disimpan ("*Form*" *concept*) dan yang dihapus dari penyimpanan beserta alasan dihapus (*"Log Info" concept*). Tugas lainnya terkait dengan tahap presentasi termasuk mematikan komputer dengan benar atau barang bukti, Mengangkut bukti ke lokasi yang aman dan membatasi akses ke bukti asli, ditemukan dalam *"Procedures", "Forms "* dan *"Log Info" concept,* masing-masing. Seperti diagram konsep pelestarian di bawah ini;



Gambar 2. 4 Peta konsep pelestarian barang bukti

(Tanner & Dampier, 2009).

2.4.2 Aturan Barang Bukti

Barang bukti harus memiliki hubungan yang relevan dengan kasus yang ada. Dalam peraturan barang bukti, terdapat empat persyaratan:

1. Dapat diterima (*admissible*) oleh hukum;
2. Asli (*authentic*) dengan kasus yang terjadi dan bukan rekayasa;
3. Lengkap (*complete*) terdapat banyak petunjuk yang dapat membantu proses penyelidikan.
4. Dapat dipercaya (*believable/reliable*), sehingga bukti dapat mengatakan hal yang terjadi di belakangnya.

2.4 Obyek Forensika Digital

Dalam dunia kriminal dikenal istilah “tidak ada kejahatan yang tidak meninggalkan jejak”. Beberapa “jejak” yang ditinggalkan oleh tindakan kejahatan menggunakan teknologi komputer. (Eko Indrajit, 2014)

1. Log *file* atau catatan aktivitas penggunaan komputer yang tersimpan secara rapi dan detail di dalam sistem;

2. *File* yang sekilas telah terhapus secara sistem, namun secara teknikal masih bisa diambil dengan cara-cara tertentu;
3. Catatan digital yang dimiliki oleh peranti pengawas trafik seperti IPS (*Intrusion Prevention System)* dan IDS (*Intrusion Detection System*);
4. *Hard disk* yang berisi data/informasi backup dari sistem utama;
5. Rekaman email, *mailing list*, blog, chat, dan mode interaksi dan komunikasi lainnya;
6. Beraneka ragam jenis berkas *file* yang dibuat oleh sistem maupun aplikasi untuk membantu melakukan manajemen *file* (misalnya: *.tmp*, *.dat*, *.txt*, dan lain-lain);
7. Rekam jejak interaksi dan trafik via internet dari satu tempat ke tempat yang lain (dengan berbasis IP *address* misalnya);
8. Absensi akses Server atau komputer yang dikelola oleh sistem untuk merekam setiap.
9. Adanya pengguna yang *login* ke peranti terkait; dan lain sebagainya.

Berikut beberapa contoh obyek forensika digital yaitu (Al-azhar, 2012):

1. *Logical file*, yaitu *file-file* yang masih ada dan tercatat di *file Systems* yang sedang berjalan (*running*) di suatu partisi. *File-file* tersebut bisa berupa *file-file* aplikasi, *library, office, logs,* multimedia dan lain-lain.
2. *Deleted file*, dikenal juga dengan istilah *unallocated cluster* yang merujuk pada *cluster* dan sektor tempat penyimpanan *file* yang sudah terhapus dan tidak teralokasikan lagi untuk *file* tersebut dengan ditandai dalam *file system* sebagai area yang dapat digunakan lagi untuk penyimpanan *file-file* baru. Artinya *file* yang sudah terhapus tersebut masih tetap berada di *cluster* atau sektor tempat penyimpanannya sampai tertimpa (*overwritten*) oleh *file-file* yang baru pada *cluster* atau sektor tersebut. Pada kondisi di mana *deleted file* tersebut belum tertimpa, maka proses *recovery* secara utuh terhadap *file* tersebut sangat memungkinkan terjadi.

3. *Lost file*, yaitu *file* yang sudah tidak tercatat lagi di *file system* yang sedang berjalan (*running*) dari suatu partisi, namun *file* tersebut masih ada di sektor penyimpanan. Ini bisa terjadi ketika misalnya suatu *flash disk* atau *hard disk* maupun partisinya dilakukan proses re-format yang menghasilkan *file system* yang baru, sehingga *file-file* yang sudah ada sebelumnya menjadi tidak tercatat lagi di *file system* yang baru. Untuk proses *recovery*-nya didasarkan pada *signature* dari *header* maupun *footer* yang tergantung pada jenis format *file* tersebut.
4. *File slack*, yaitu sektor penyimpanan yang berada di antara *End of File* (EoF) dengan *End of Cluster* (EoC). Wilayah ini sangat memungkinkan terdapat informasi yang mungkin penting dari *file-file* yang sebelumnya sudah dihapus (*deleted*).
5. *Log file*, yaitu *file-file* yang merekam aktivitas (*logging*) dari suatu keadaan tertentu, misalnya *log* dari sistem operasi, *internet browser*, aplikasi, *internet traffic* dan lain-lain.
6. *Encrypted file*, yaitu *file* yang isinya sudah dilakukan enkripsi dengan menggunakan algoritma kriptografi yang kompleks sehingga tidak bisa dibaca atau dilihat secara normal. Satu-satunya cara untuk membaca atau melihatnya kembali adalah dengan melakukan deskripsi terhadap *file* tersebut menggunakan algoritma yang sama. Ini biasa digunakan dalam dunia digital *information security* untuk mengamankan informasi yang penting. Ini juga merupakan salah satu bentuk dari anti forensik, yaitu suatu metode untuk mempersulit ahli forensika digital mendapatkan informasi mengenai jejak-jejak kejahatan.
7. *Steganography file*, yaitu *file* yang berisikan informasi rahasia yang Disisipkan ke *file* lain, biasanya berbentuk *file* gambar, video atau Audio, sehingga *file-file* yang bersifat *carrier* (pembawa pesan rahasia) tersebut terlihat normal dan wajar bagi orang lain, namun bagi orang yang tahu metodologinya, *file-file* tersebut memiliki makna yang dalam dari informasi rahasia tersebut. Ini juga dianggap sebagai salah satu bentuk anti forensik.

8. *Office file*, yaitu *file-file* yang merupakan produk dari aplikasi Office, Seperti Microsoft Office, Open Office dan sebagainya. Ini biasanya berbentuk *file-file* dokumen, *spreadsheet, database,* teks dan presentasi.
9. *Audio file*, yaitu *file* yang berisikan suara, musik dan lain-lain, yang biasanya berformat *wav* dan *mp3* dan sebagainya. *File* audio yang berisikan rekaman suara percakapan orang ini biasanya menjadi penting dalam penyelidikan ketika suara di dalam *file* audio tersebut perlu diperiksa dan dianalisis secara audio forensik untuk memastikan suara tersebut apakah sama dengan suara pelaku kejahatan.
10. *Video file,* yaitu *file* yang memuat rekaman video, baik dari kamera digital, *handphone, handy cam* maupun CCTV. *File* video ini sangat memungkinkan memuat wajah pelaku kejahatan sehingga *file* ini perlu dianalisis secara detail untuk memastikan bahwa yang ada di *file* tersebut adalah pelaku kejahatan.
11. *Image file,* yaitu *file* gambar digital yang sangat memungkinkan memuat informasi-informasi yang penting yang berkaitan dengan kamera dan waktu pembuatannya (*time stamps*). Data-data ini dikenal dengan inisial metadata *EXIF* (*exchangeable image file*). Meskipun begitu, meta data *exif* ini bisa dimanipulasi, sehingga ahli forensika digital atau investigator harus hati-hati ketika memeriksa dan menganalisis meta data dari *file* tersebut.
12. *Email* (*electronic mail*), yaitu surat berbasis sistem elektronik yang menggunakan sistem jaringan online untuk mengirimkannya atau menerimanya. *Email* menjadi penting di dalam penyelidikan khususnya *phishing* (yaitu, kejahatan yang menggunakan *email* palsu dilengkapi dengan identitas palsu untuk menipu si penerima). *Email* berisikan *header* yang memuat informasi penting jalur distribusi pengiriman *email* mulai dari pengiriman (*sender*) sampai di penerima (*recipient*). Oleh karena itu, data di *header* inilah yang sering dianalisis secara teliti untuk memastikan lokasi si pengirim yang didasarkan pada alamat IP. Meskipun begitu, data-data di *heade*r juga sangat dimungkinkan untuk dimanipulasi. Dengan

demikian, pemeriksaan *header* dari *email* harus dilakukan secara hati-hati dan komprehensif.

13. *User ID* dan *password*, merupakan syarat untuk masuk ke suatu akun secara online. Jika salah satunya salah, maka akses untuk masuk ke akun tersebut akan ditolak.
14. *Short Message Service (SMS)*, yaitu layanan pengiriman dan penerimaan pesan pendek yang diberikan oleh operator seluler terhadap pelanggan nya SMS-SMS yang bisa berupa SMS masuk (*inbox*), keluar (*sent*) dan rancangan (*draf*) dapat menjadi petunjuk dalam penyelidikan untuk mengetahui keterkaitan antara pelaku yang satu dengan yang lain.
15. *Multimedia Message Service (MMS)*, merupakan jasa layanan yang diberikan oleh operator seluler berupa pengiriman dan penerimaan pesan multimedia yang bisa berbentuk suara, gambar atau video.
16. *Call logs*, yaitu catatan panggilan yang terekam pada suatu nomor panggil seluler. Panggilan ini bisa berupa *incoming* (panggilan masuk), *outgoing* (panggilan keluar) dan *missed call* (panggilan tak terjawab)

2.5 Pemodelan Forensika Digital

Model forensika digital melibatkan tiga komponen terangkai yang dikelola sedemikian rupa hingga menjadi sebuah tujuan akhir dengan segala kelayakan dan hasil yang berkualitas. Ketiga komponen tersebut adalah komponen ini mencakup manusia (*people*), peralatan/perangkat (*device*) dan aturan (*protocol*) yang dirangkai, di berdayakan dan dikelola sedemikian rupa dalam mencapai tujuan akhir dengan segala kelayakan dan kualitas.(“Metode Komputer Forensik,” 2012)

Gambar 2. 5 Ilustrasi Komponen Forensika Digital

1. Manusia *(People),* diperlukan kualifikasi untuk mencapai manusia yang berkualitas. Memang mudah untuk belajar komputer forensik, tetapi untuk menjadi ahlinya, dibutuhkan lebih dari sekadar pengetahuan dan pengalaman.
2. Peralatan *(Equipment),* diperlukan sejumlah perangkat atau alat yang tepat untuk mendapatkan sejumlah bukti *(evidence)* yang dapat dipercaya dan bukan sekadar bukti palsu.
3. Aturan *(Protocol),* diperlukan dalam menggali, mendapatkan, menganalisis, dan akhirnya menyajikan dalam bentuk laporan yang akurat. Dalam komponen aturan, diperlukan pemahaman yang baik dalam segi hukum dan etika, kalau perlu dalam menyelesaikan sebuah kasus perlu melibatkan peran konsultasi yang mencakup pengetahuan teknologi informasi dan ilmu hukum.

2.6 Kebutuhan Sumber Daya

Untuk melakukan aktivitas forensik, dibutuhkan teknik dan peranti bantu forensik (*software dan hardware*). Peranti lunak atau *software* digunakan untuk membantu ahli forensika digital dalam melakukan hal-hal sebagai berikut: (Eko Indrajit, 2014)

1. Mencari dan mengembalikan *file* yang telah terhapus sebelumnya;

2. Membantu merekonstruksi pecahan-pecahan *file* yang ada (*corrupted file*);
3. Mengidentifikasi anomali program melalui analisa serangkaian data beserta struktur algoritma yang terdapat pada sebuah *file* atau sistem basis data;
4. Menemukan jejak-jejak yang tertinggal dalam sebuah peristiwa kriminal tertentu yang telah dilakukan sebelumnya;
5. Mendapatkan data berbasis pola-pola tertentu sesuai dengan permintaan penegak hukum dalam proses investigasi peristiwa kejahatan internet;
6. Memfilter dan memilah antara data yang berguna/relevan untuk kebutuhan forensik dengan yang tidak, agar mekanisme analisa dapat dilakukan secara fokus dan detail;
7. Menganalisa kejanggalan-kejanggalan yang terdapat pada suatu program atau sub program tertentu;
8. Mempercepat proses pencarian penggalan instruksi atau data tertentu yang dibutuhkan oleh seorang ahli forensik terhadap sebuah media *repository* bermemori besar;
9. Menguji dan mengambil kesimpulan terhadap sejumlah kondisi tertentu terkait dengan aktivitas dan konsep forensik; dan lain sebagainya.

Selain peranti lunak, peranti keras juga diperlukan agar proses forensik dapat dilakukan secara efektif dan sesuai dengan prosedur standar yang berlaku. Peranti keras digunakan untuk:

1. Membuat replikasi atau copy atau *cloning* yang identik;
2. Mengambil atau memindahkan atau mengekstrak data dari tempat-tempat atau media penyimpan yang khusus seperti: telepon genggam, server besar (super komputer), PDA (*Personal Digital Assistance*), komputer tablet, dan lain-lain;
3. Menggenerasi nilai numerik secara urut maupun random secara ultra cepat guna pemecahan sandi / kode;
4. Membongkar proteksi secara peranti keras atau lunak;
5. Menghapus atau memformat *hard disk* secara cepat dan efektif.

2.7 Komparasi

Standar Operating Procedure (SOP) yang disusun oleh Pusat Laboratorium Forensik Polisi RI dalam menangani barang bukti digital antara satu kategori dengan kategori lainnya memiliki kesamaan atau memiliki tahapan yang sama. Terdapat 15 SOP dalam menangani setiap barang bukti elektronik dan/atau barang bukti digital (Al Azhar, 2013):

1. SOP 1 tentang prosedur analisa forensik digital
2. SOP 2 tantang komitmen jam kerja
3. SOP 3 tentang pelaporan forensik digital
4. SOP 4 tentang menerima barang bukti elektronik dan/atau digital
5. SOP 5 tentang penyerahan kembali barang bukti elektronik dan/atau digital
6. SOP 6 tentang triage forensik (penanganan awal barang bukti di TKP)
7. SOP 7 tentang akuisisi langsung
8. SOP 8 tentang akuisisi *hard disk, flash disk* dan *memory card*
9. SOP 9 tentang analisa *hard disk, flash disk* dan *memory card*
10. SOP 10 tentang akuisisi ponsel dan *sim card*
11. SOP 11 tentang analisa ponsel dan *sim card*
12. SOP 12 tentang analisa forensik audio
13. SOP 13 tentang analisa forensik video
14. SOP 14 tentang analisa gambar digital
15. SOP 15 tentang analisa forensik jaringan

Barang bukti elektronik dan/atau digital menurut Puslabfor Polri dibagi menjadi 6 kategori pemeriksaan dan analisa:

1. *Hard disk*, flash disk dan *memory card*
2. Ponsel dan *sim card*
3. Forensik audio
4. Forensik video
5. Forensik gambar digital
6. Forensik jaringan

Tabel komparasi SOP penanganan barang bukti elektronik dan/atau barang bukti digital sesuai SOP 1 dapat dilihat pada Tabel di bawah ini.

Barang bukti elektronik dan/atau Digital	Standar Operasional Prosedur														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Hard disk, flashdisk dan memory card			d	a	e			b	c						
Ponsel dan *simcard*			d	a	e					b	c				
Forensik Audio			d	a	e			b				c			
Forensik video			d	a	e			b					c		
Forensik gambar digital			d	a	e			b						c	
Forensik jaringan			d	a	e			b							c

Tabel 2.1 Komparasi Penanganan Barang Bukti Digital

2.8 Manajemen Kasus

Manajemen kasus memainkan peran penting, dalam mengikat semua kegiatan dan hasil dari penyelidikan digital. Tujuan dari manajemen kasus yang efektif adalah untuk memastikan bahwa penyelidikan digital berlangsung lancar serta semua informasi yang dihasilkan relevan dari setiap tahapan dari proses yang dikerjakan dan didokumentasikan, sehingga menghasilkan gambaran yang jelas dari peristiwa yang berkaitan untuk suatu pelanggaran atau insiden. Efektivitas penyelidikan digital sangat tergantung pada kasus manajemen terutama saat melacak barang bukti, peristiwa dan temuan forensik.

Selain itu, manajemen kasus melibatkan komunikasi dan berbagi prioritas, termasuk informasi antara ahli forensik, serta mendelegasikan tugas-tugas administrasi di antara beberapa ahli forensik digital dalam investigasi digital (Casey & Schatz, 2011).

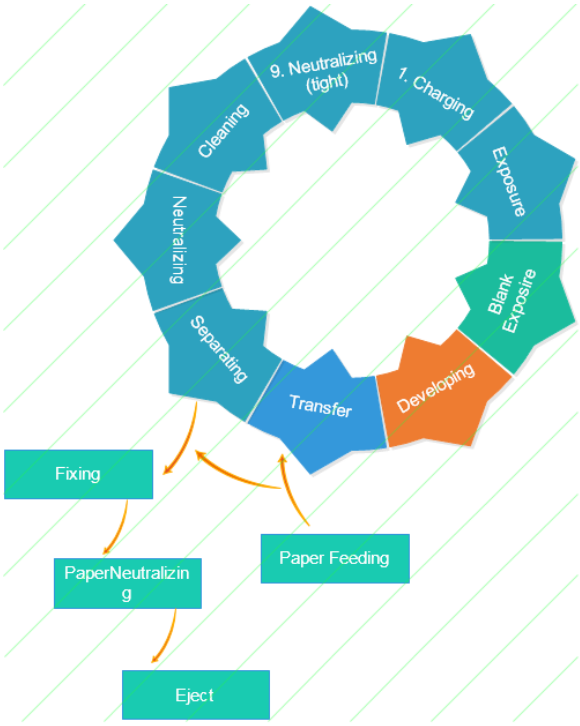
2.9 Mesin Fotokopi

Penggunaan mesin fotokopi menjadi sebuah teknik modern yang dimulai pada awal abad ke-20, sejak saat itu fotokopi menjadi teknik yang paling populer dalam upaya mereproduksi dokumen. Mesin fotokopi dikenal sebagai sebuah perangkat yang berfungsi untuk memperbanyak kertas dokumen dan lainnya. *Encyclopedia Britania* memberi definisi mesin fotokopi sebagai suatu alat untuk

menyalin kembali dokumen atau ilustrasi dengan menggunakan cahaya, panas, bahan kimia atau muatan listrik statis (Encyclopaedia Britania, 2014). Mesin fotokopi pertama ditemukan oleh Chaster F. Carison, seorang ahli fisika Amerika pada tahun 1939. Mesin fotokopi klasik menggunakan energi listrik statis untuk menggandakan naskah yang dinamakan Xerography. Xerography artinya tulisan kering (Wikipedia, 2014) Mesin fotokopi juga dikenal sebagai perangkat untuk menyalin kembali dokumen atau ilustrasi dengan menggunakan cahaya, panas, bahan kimia atau muatan listrik statis yang berfungsi untuk memperbanyak kertas dokumen dan lainnya (Encyclopaedia Britania, 2014).

2.10.1 Prinsip Dasar Kerja Mesin fotokopi

Sebelum dimulainya integrasi komputerisasi pada mesin fotokopi pada tahun 2002 (CBSNews, 2010). Proses kinerja mesin fotokopi dapat dilihat pada diagram di bawah ini.

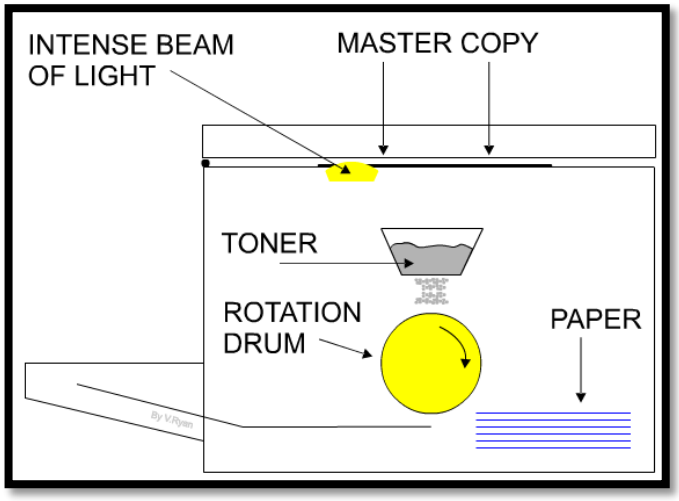


Gambar 2. 6 Diagram Proses penyalinan pada mesin fotokopi (Poentoadji, 1990)

Kinerja mesin fotokopi pada dasarnya meliputi dua buah siklus dari saat dihidupkan hingga proses penyalinan dilakukan, siklus tersebut adalah proses pemanasan dan proses penyalinan (Poentoadji, 1990).

1. Proses pemanasan merupakan proses pemanasan yang terjadi pada mesin yang dilakukan oleh *fuser roller heater* guna memanaskan *fixing roller* sesuai temperatur yang diinginkan. *Fixing roller* adalah rol dalam toner laser printer yang akan meleleh di atas kertas (Virtualizationadmin, 2014).
2. Siklus penyalinan merupakan proses penyalinan yang dilakukan oleh mesin. Proses penyalinan terdapat 13 tahap proses kerja dari mulai proses penggambaran hingga pemindahan penggambaran ke media cetak.

V. Ryan menjelaskan alur kerja sederhana dari mesin fotokopi (Ryan, 2010);



Gambar 2. 7 Diagram kerja mesin fotokopi oleh V. Ryan

(sumber: http://technologystudent.com/designpro/prtpro6.htm)

1. Pertama-tama, kita meletakkan kertas master yang hendak kita fotokopi di mana bagian yang ingin di fotokopi dihadapkan ke bawah.
2. Cahaya reflektor akan melakukan fungsi *scanning* untuk menangkap gambaran dari lembar master.

3. Kemudian toner akan bereaksi secara otomatis sehingga “menumpahkan” tinta ke bagian drum, di mana tinta yang ditumpahkan ini sudah sesuai dengan hasil *scan* di langkah nomor 2.
4. Drum yang telah tertuang tinta tersebut kemudian berputar dan otomatis mencetak hasil *scan* di nomor 2 di permukaan kertas yang telah tersedia di mesin fotokopi tersebut.

2.10.2 Mesin Fotokopi *Multi Function Peripheral* (MFP)

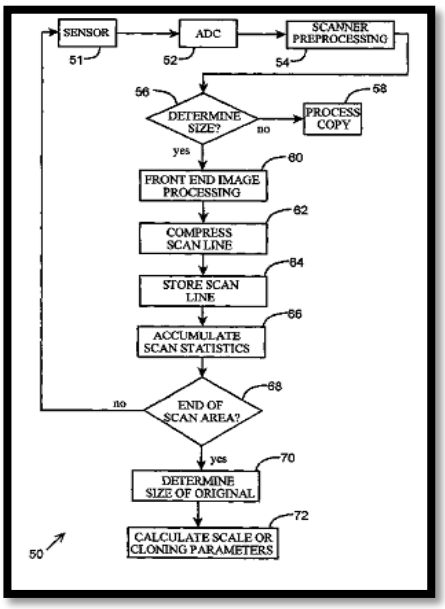
Multi Function Peripheral (MFP) berhubungan dengan perangkat multi fungsi dari mesin fotokopi digital dan lebih khusus sebagai teknik untuk meningkatkan fungsi dari mesin fotokopi konvensional atau melakukan operasi khusus. *Multi Function Peripheral* atau perangkat Multi fungsi adalah perangkat yang mampu melakukan berbagai fungsi dari fungsi-fungsi perangkat terpisah (Whatls.com, 2014).

Sebagai aturan, sebuah perangkat MFP harus memiliki fungsi sedikitnya dua dari alat berikut (Technopedia, 2014):

- *Printing*
- *Copying*
- *Scanning*
- *Faxing*
- *Stapling*
- *Duplexing*
- *Hole punching*
- *Color and/or black and white printer compatibility*
- *Extra paper trays*
- *Photo organization software*
- *Optical character recognition software*
- *A USB or parallel port*

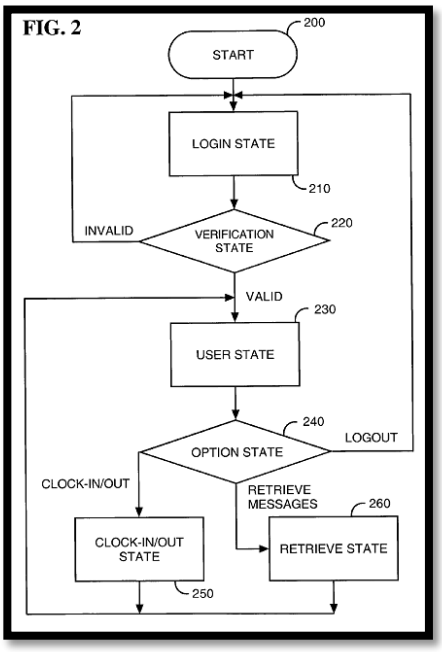
Perangkat mesin fotokopi digital MFP dapat melakukan fungsi khusus termasuk merekonstruksi dokumen yang dicetak, seperti skala dan pengukuran otomatis terhadap ukuran salinan ke media lain. Fungsi khusus lainnya adalah menyalin *auto-cloning*, di mana mesin fotokopi menghasilkan beberapa gambar "kecil ". Gambar asli tersusun pada selembar media salinan (L.Levin, Dalrymple, & Dolan, 2007).

Sebuah paten oleh Seiichi Katano, mengatakan mesin fotokopi digital MFP merupakan sebuah perangkat yang dapat melakukan beberapa fungsi. Mesin MFP dilengkapi untuk tampil sebagai printer, *scanner*, faksimile mesin, dan mesin fotokopi. sebuah perangkat input/output yang dikonfigurasi dengan perangkat penyimpanan (*Hard disk*) serta dapat melakukan berbagai tugas, fungsi dan aplikasi (Katano, 2004). Katano menambahkan bahwa mesin MFP dapat mencatat waktu dari aktivitas yang dilakukan pengguna kepada perangkat tersebut. Selanjutnya, jika ada pesan (*message*) yang diterima, maka pesan tersebut langsung tersimpan pada tempat penyimpanan data yang dapat dioperasikan melalui server jarak jauh.



Gambar 2. 8 Diagram Blok dari mesin fotokopi digital.

(L.Levin et al., 2007)



Gambar 2. 9 Diagram yang menggambarkan operasi MFP yang mungkin melakukan berbagai fungsi (Katano, 2004)

2.10 Joint Bi-Level Group (JBG)

JBG merupakan file ekstensi dengan tipe file JBIG. JBG atau yang dikenal juga dengan JBIG adalah standar kompresi gambar lossless dari *Joint Bi-level Image Experts Group* dan telah terstandarisasi ISO/IEC 11544 dan direkomendasi oleh ITU-T rekomendasi T.82 yang banyak diterapkan di mesin FAX dan Fotokopi MFP. JBIG dirancang untuk kompresi gambar biner terutam untuk fak dan mesin fotokopi tetapi juga dapat digunakan untuk gambar lain JBIG didasarkan pada bentuk aritmetika *coding* dipatenkan oleh IBM, yang dikenal sebagai *Q-coder*, tetapi menggunakan *tweak* kecil dipatenkan oleh Mitsubishi, sehingga juga dikenal sebagai *QM-coder* (Kuhn, 2002).

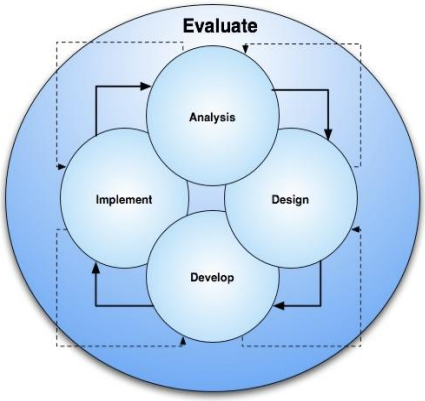
BAB III

METODOLOGI PENELITIAN

3.1 Metode Penelitian

Metode yang digunakan pada penelitian ini adalah metode penelitian dan pengembangan (*Research and Development*) dengan model ADDIE (*Analysis, Design, Development, Implementation, Evaluation*). Model ADDIE diasaskan oleh Rosset pada tahun 1987, merupakan model reka bentuk yang berfungsi sebagai garis panduan ke arah proses yang menyediakan sarana untuk pengambilan keputusan untuk menentukan siapa, apa, kapan, di mana, mengapa, dan bagaimana sebuah program penelitian tersebut. Konsep pendekatan sistem didasarkan pada perolehan keseluruhan gambaran dari proses penelitian. Hal ini ditandai dengan proses teratur untuk mengumpulkan dan menganalisis persyaratan kinerja kolektif dan individu dan kemampuan untuk merespons kebutuhan yang teridentifikasi (Clark, 2014).

Metode ini digunakan dalam penelitian teknik akuisisi artifak digital pada perangkat mesin fotokopi MFP serta membangun kerangka kerja bagi investigator khusus investigasi pelanggaran yang menggunakan perangkat mesin fotokopi MFP. Penelitian dilakukan pada perangkat mesin fotokopi *Multi Function Peripheral* merek Canon seri iR6000. Penelitian membutuhkan beberapa tahapan yang sistematik, runut dan memiliki keterkaitan antara komponen yang satu dengan yang lainnya. Adapun tahapan model AADIE (Prasetyo, 2012).



Gambar 3. 1 Instructional System Design

1. Tahap *Analysis* adalah dasar dari proses penelitian yang mencakup: Studi pendahuluan dan mengidentifikasi tujuan. Seluruh hasil dari tahap ini dikirimkan untuk semua kegiatan desain dan pengembangan selanjutnya.
   a. Kebutuhan penelitian yang diperlukan.
   b. Apa yang mesti diteliti.
   c. Bagaimana proses penelitian.
   d. Standar kerja
   e. Siapa tujuan hasil diperuntukkan
2. Tahap *Design* mencakup strategi perencanaan untuk mencapai tujuan, tahapan ini menjamin gambaran yang sistematis dari proses penelitian.
3. Tahap *Development* meliputi persiapan teknis, alat-alat penelitian, akuisisi digital dan rancangan pengembangan kerangka kerja,
4. Tahap *Implementasi* meliputi kegiatan dalam pengerjaan penelitian, seperti akuisisi, analisis data digital, pembuatan kerangka kerja serta pembuatan laporan,
5. Evaluasi mencakup formatif dan evaluasi sumatif.

   Evaluasi formatif merupakan proses evaluasi berbasis proses sedangkan evaluasi sumatif merupakan evaluasi yang berfokus pada hasil akhir.

Hasil akhir dari penelitian ini adalah laporan hasil penelitian dan kerangka kerja yang dirancang sebagai pedoman akuisisi perangkat mesin fotokopi *Multi Function Peripheral* (MFP).

3.1.1 Analisis Kebutuhan

Analisis kebutuhan dilakukan dengan melakukan studi pendahuluan guna mencari informasi untuk mempertajam arah penelitian serta kemungkinan diteruskannya pekerjaan meneliti dan mencari informasi yang diperlukan oleh peneliti agar masalah menjadi jelas kedudukannya. Secara umum studi pendahuluan dilakukan dengan mengumpulkan informasi melalui:

1. *Paper* (Studi Literatur): Meliputi dokumen, buku, majalah atau bahan tertulis lainnya, baik berupa teori, laporan penelitian atau penemuan sebelumnya baik bersifat *online source* maupun *offline source.*
2. *Person* : Dilakukan dengan cara bertemu, bertanya dan berkonsultasi dengan para ahli.
3. *Place:* Berupa tempat, lokasi atau benda-benda yang terdapat di tempat penelitian.

3.1.2 Desain dan Pengembangan

Pada tahap desain dan pengembangan, dilakukan dengan perencanaan yang sistematis dan bertahap.

1. Pengamatan objek penelitian

   Objek penelitian yaitu perangkat mesin fotokopi MFP Canon iR6000 khususnya lokasi media penyimpanan *non-volatile*. Tahapan ini dilakukan bertujuan untuk mendapatkan informasi dari objek yang diteliti.
2. Pemodelan forensika digital

   Tahapan ini menerapkan teknik-teknik, model serta aturan yang akan digunakan pada objek penelitian menurut kesesuaiannya. Pada tahap ini juga dirumuskan suatu rencana akuisisi serta pemeriksaan pada mesin fotokopi secara fisik

3. Perancangan pemodelan

   Tahapan ini perancangan Kerangka investigasi dilakukan baik secara teknik, kebutuhan serta aturan berdasarkan data-data pada pemodelan forensika komputer.

3.1.3 Implementasi

Implementasi dilakukan dengan mengikuti model yang didapat pada tahap sebelumnya. Implementasi dalam penelitian ini berbentuk pengerjaan akuisisi baik secara fisik maupun digital yang dilakukan pada perangkat. Perancangan pembuatan Kerangka kerja penyelidikan mesin fotokopi MFP dilakukan setelah seluruh proses akuisisi pada perangkat dianggap selesai.

3.1.4 Evaluasi

Hasil akhir dari penelitian ini berupa laporan penelitian secara keseluruhan serta prosedur baru penanganan forensika digital perangkat mesin fotokopi MFP, yang nantinya akan dievaluasi serta direvisi oleh pihak yang dianggap kompeten dalam bidang forensika digital.

3.2 Canon *Image* Runner (iR) 6000

Mesin fotokopi Canon model iR6000 dirancang guna memanfaatkan kekuatan jaringan pelanggan untuk merampingkan manajemen informasi. Canon iR6000 dibangun berdasarkan Platform produk digital Canon, menawarkan kemampuan tradisional dan baru untuk kelompok kerja perusahaan dan departemen. Canon iR6000 memiliki kemampuan mencetak, menyalin dan memindai melalui koneksi jaringan *Local Area Networks* (LAN). Pengaturan oleh pengguna dapat dilakukan dengan antarmuka yang *user friendly* langsung dari komputer pengguna.

Selain kemampuan pencetakan melalui koneksi jangarin, iR6000 juga dilengkapi dengan fungsi baru.

- *Confidential Printing:* Izin masuknya tujuh digit PIN rahasia dari dalam *image* RUNNER 6000. Dokumen dikirim ke perangkat dan dicetak pada saat dimulainya nomor rahasia pengguna PIN pada perangkat.
- *Mail box Printing*: Pengguna dapat mencetak ke *email* pribadi untuk integrasi dengan dokumen lain yang sebelumnya dicetak atau dipindai ke kotak surat mereka, sehingga menciptakan dokumen senyawa baru.
- *In-line Finishing*: Langsung dari iR6000 desktop, pengguna dapat dengan mudah dan langsung mengakses ke semua pilihan penyelesaian pada iR6000.
- *Job Accounting*: Ketika dilengkapi dengan opsional NetSpot ® Akuntan * perangkat lunak, iR6000 dapat menangkap pelacakan informasi pekerjaan/pengguna dengan tujuan penagihan.

Gambar 3. 2 Tampilan Canon *image* Runner (iR) 6000

Sumber: http://copysolution.biz/view.php?id=8

3.3 Proses Investigasi Forensika Digital Pada Objek Penelitian (Canon iR6000)

Proses investigasi forensika digital pada objek penelitian ditempuh setelah didapat data yang cukup valid dari proses studi analisis hingga proses desain dan pengembangan kerja. Tujuan utama dari investigasi yaitu guna mengikuti jejak yang ditinggalkan pelaku selama proses kejahatan yang nanti nya digunakan untuk mengungkap hubungan antara pelaku, korban dan Tempat Kejadian Perkara (TKP) (Carrier & Spafford, 2003).

Proses ini melakukan evaluasi secara menyeluruh dengan meninjau sifat perangkat keras, perangkat lunak, artifak potensial dan keadaan sekitar objek penelitian.

3.3.1 Model Investigasi

Model investigasi dibedakan pada dua buah tahapan tujuan guna mendapatkan barang bukti yaitu tahapan lingkungan fisik (*physical*) dan lingkungan virtual (*digital*) (Casey & Schatz, 2011). Lingkungan fisik (*physical*) merupakan di mana bukti fisik kejahatan tersebut didapat (TKP) sedangkan lingkungan virtual (*digital*) merupakan di mana bukti digital tersebut dibuat atau tercipta dari perangkat lunak atau perangkat keras yang ada di lingkungan fisik.

	(PHASE GOAL) PHYSICAL	PHASE GOAL DIGITAL
Pelestarian TKP	Mengamankan pintu masuk dan keluar serta mencegah perubahan fisik bukti	Mencegah perubahan potensial bukti digital, termasuk isolasi jaringan, mengumpulkan volatil data, dan menyalin seluruh lingkungan digital
Penelitian TKP	Mengikuti alur tema kasus, mengidentifikasi keseluruhan bukti fisik	Identifikasi barang bukti nyata menggunakan pencarian bukti digital (biasanya di laboratorium)

	(PHASE GOAL) PHYSICAL	PHASE GOAL DIGITAL
Dokumentasi TKP	Foto-foto, sketsa, peta bukti, dan TKP	Foto-foto perangkat digital dan deskripsi dari masing-masing perangkat digital
Pencarian dan pengumpulan TKP	Pencarian yang mendalam untuk barang bukti fisik	Analisis sistem untuk bukti yang belum jelas (biasanya di laboratorium)
Rekontruksi TKP	Mengembangkan teori berdasarkan hasil analisis dan pengujian terhadap bukti	

Tabel 3.1 Tahapan investigasi fisik dan digital pada model proses investigasi Carrier

3.3.2 Persiapan Umum

Fase ini dilakukan guna mengetahui benar, saat menentukan tindakan terkait objek penelitian dan lingkup kerja yang akan diselesaikan. Beberapa fase proses persiapan umum yang akan dilakukan adalah.

1. Menentukan tujuan kerja penelitian,
2. Mengidentifikasi perangkat MFP yang dihadapi,
3. Mengidentifikasi koneksi jaringan pada perangkat,
4. Mengidentifikasi dan mendokumentasi jenis, konfigurasi perangkat lunak pada objek penelitian.
5. Mengidentifikasi dan mendokumentasi perangkat fisik serta lokasi penyimpanan data (*hard disk*).
6. Menentukan kesesuaian kebutuhan guna akuisisi perangkat. Kebutuhan dapat berupa peralatan dan media pemeriksaan.
7. Mencatat keterangan pada objek penelitian.
8. Menentukan jenis tindakan dan urutan kerja.

3.3.3 Penanganan Objek Penelitian (Canon iR 6000)

Bukti digital pada dasarnya adalah rapuh dan mudah di rubah, di rusak atau dihancurkan oleh penanganan yang tidak tepat. Oleh sebab itu penelusuran data harus dilakukan dengan prosedur dan tahapan yang jelas dan sistematika, sehingga integritas data dapat terjamin. Prosedur awal yang dilakukan adalah dengan melakukan persiapan administrasi investigasi/penelitian serta peralatan-peralatan pendukung, seperti melakukan pencatatan dan foto forensik.

Pada penelitian ini akuisisi objek penelitian dilakukan dalam dua kondisi keadaan:

1. Perangkat dalam keadaan menyala (On).
   Tahapan-tahapan yang dikerjakan ketika kondisi perangkat menyala atau tersambung arus listrik dilakukan dua lokasi pemeriksaan.
   a. Perangkat mesin fotokopi
   b. Perangkat komputer yang terkoneksi mesin
2. Perangkat dalam keadaan padam (Off)
   Tahapan-tahapan yang dikerjakan ketika mesin dianggap dalam kondisi padam (Off).

3.3.4 Akuisisi Langsung (*Live Acquisition*) Pada Objek Penelitian

Akuisisi Langsung (*Live Acquisition*) mengacu pada kegiatan-kegiatan yang semestinya dilakukan oleh ahli forensika digital ketika menemukan barang bukti dari perangkat objek penelitian dalam keadaan menyala (*power on*). Prinsip dari kegiatan ini adalah usaha untuk mendapatkan data-data investigatif seefesien mungkin (cepat dan tepat) dengan perubahan isi *hard disk* seminim mungkin. Akuisisi artifak dapat dilakukan secara langsung pada objek penelitian dan/atau pada komputer yang di/terkoneksi pada perangkat tersebut.

3.3.5 Akuisisi Tidak Langsung (*Static Acquisition*) Perangkat Penyimpanan *Non-Volatile*

Akuisisi mengacu pada serangkaian prosedur pengambilan material dari perangkat objek penelitian dalam keadaan padam (*Power off*). Pengambilan material/artifak dilakukan dengan menerapkan langkah-langkah penanganan guna menjaga integritas dari objek penelitian tersebut. Akuisisi dilakukan dengan memisahkan media penyimpanan *non-volatile* dari perangkat Canon iR 6000. Proses Akuisisi memiliki beberapa tahapan umum yaitu *Imaging* (Duplikasi), *Hasing*, Ekstraksi dan Analisis.

3.3.5.1 Forensik Imaging

Duplikasi atau yang dikenal dengan istilah *forensik imaging* pada forensika digital merupakan teknik menggandakan barang bukti secara identik. Duplikasi menggunakan serangkaian prosedur, guna memastikan integritas hasil dan sumber, dengan kata lain *forensik imaging* merupakan proses memetakan penggandaan barang bukti dan dilakukan dengan metode bit by bit copy.

3.3.5.2 Forensik Hasing

Hashing dilakukan guna mengetahui derajat kesamaan pada sumber asli dari hasil duplikasi. Nilai *hashing* tidak sama maka *forensik imaging* harus diulangi. Setelah proses *forensik imaging* selesai dan menghasilkan *image file*, maka hasil *image file* tersebut diperiksa untuk kecocokan nilai *hash* MD5. Oleh sebab itu, awal pemeriksaan *hashing* mesti dilakukan pada *hard disk* sumber, selanjutnya *hashing* dilakukan pada *image file* dari hasil *forensik imaging.*

3.3.5.3 Forensik Ekstraksi

Forensik ekstraksi merupakan proses di mana data diambil atau di ekstrak dari file hasil *forensik imaging* baik menggunakan *query* atau *tool forensik analysis.*

3.3.5.4 Forensik Analisis

Setelah mendapatkan *file-file* atau artifak digital yang diinginkan dari proses penyelidikan, selanjutnya dipilah-pilah sesuai perkiraan hubungan artifak dengan kepentingan penelitian. Artifak yang berhubungan dianalisis menggunakan *tool forensik analysis* untuk mengetahui meta data, waktu, *log* pengguna, serta bagaimana data tersebut dapat di proses, dibaca dan dimengerti oleh ahli forensika digital.

3.4 Skenario Kasus

Diasumsikan berdasarkan delik aduan, sebuah kantor percetakan buku CV. Cahaya Tulis, di sinyalir sebagai tempat memproduksi buku ilegal yang berjudul "Konsep Kecerdasan Buatan, Oleh: Anita Desiani & Muhammad Arhami" digeledah oleh pihak berwajib. Pengeledahan yang dilakukan pihak berwajib pada tanggal 23 September 2014 tersebut hanya menemukan buku-buku yang memiliki izin cetak ganda dan tidak menemukan sembarang buku yang diduga sebagai buku ilegal seperti yang dilaporkan. Setelah melakukan investigasi menyeluruh di dalam gedung, 14 (empat belas) unit mesin fotokopi yang diduga digunakan sebagai alat untuk mencetak ganda buku-buku tanpa izin (ilegal). Langkah penyitaan seluruh perangkat mesin fotokopi tersebut dianggap kurang efisien karena diketahui setiap mesin fotokopi berbobot sekitar 210 Kg, selain itu penyidik belum dapat memastikan perangkat mesin fotokopi yang berhubungan dalam melakukan dugaan tindak pelanggaran pembajakan buku tersebut (pasal 34 ayat 2) ("Kitab Undang-Undang Hukum Acara Pidana (KUHAP) Undang-Undang Nomor 8 Tahun 1981," 1981).

Oleh sebab itu maka di lakukanlah prosedur forensik di TKP guna pencarian bukti permulaan.

Gambar 3. 3 Diagram ilustrasi skenario kasus

3.5 Perancangan Kerangka Kerja Penyelidikan

Perancangan kerangka kerja mencakup tahapan kerja yang relevan dari setiap proses yang dilewati. Perancangan kerangka kerja investigasi forensika digital pada mesin fotokopi MFP didasari oleh pemodelan *Electronic Discovery Reference Model* (EDRM). Perancangan ini terdiri dari empat tahapan utama yaitu diawali dari proses identifikasi hingga pembuatan laporan hasil akuisisi serta sub tahapan akan mengadopsi model investigasi Carrier.

Tahapan ini juga mencakup prosedur teknis dan *by-passing* kerangka kerja analisis penyelidikan atau minimalisir berbagai fitur sistem operasi serta mempertimbangkan semua tahapan tersebut saling berhubungan hingga mendapat kesimpulan akhir.

BAB IV

HASIL DAN PEMBAHASAN

4.1 Deskripsi Umum Canon iR6000

Mesin fotokopi *image* RUNNER (iR) 6000 dibangun berdasarkan Platform produk digital Canon. iR 6000 menawarkan beberapa kemampuan seperti mendukung pencetakan melalui jaringan, menyalin, memindai baik lokal dan jaringan, memudahkan pengguna mengakses informasi manajemen baik berbentuk kertas maupun digital.

4.1.1 Mekanisme Umum Kinerja Sistem

Sistem perangkat lunak yang digunakan untuk mengontrol kinerja mesin disimpan di dalam *hard disk drive* (HDD). *Central Processing Unit* (CPU) yang terdapat pada mesin fotokopi diprogramkan untuk membaca sistem perangkat lunak dari *hard disk* dan menulis ke RAM. Mekanisme utama dari Blok pengendali dikendalikan oleh CPU pada kontrol utama PCB.

Mesin iR 6000 dilengkapi dengan *hard disk* standar yang memungkinkan penyortiran berbasis penyimpanan. Mesin ini juga mampu membuat beberapa salinan dengan hanya sekali pembacaan pada objek salinan asli. RAM dan DIMM digunakan dalam hubungannya dengan CPU dan *Hard disk* memiliki fungsi berikut:

- CPU merupakan pengontrol pengolahan *image* yang berasal dari data *image* masukan unit pembaca.
- RAM merupakan tempat penyimpanan sementara program dan data *image*.
- DIMM-ROM merupakan tempat penyimpanan sistem pengolahan program dan *boot program.*
- HDD merupakan tempat penyimpanan perangkat lunak dan data pengguna serta *image* data sebagai bagian dari fungsi kotak penyimpanan.

4.1.2 Fitur Umum Canon iR6000

Mesin fotokopi Canon seri iR 6000 memiliki tiga buah fitur utama dalam pengoperasian nya yaitu Penyalinan (*Copy*), Kotak surat (*Mail box*) dan memindai (*Scaning*).

1. Penyalinan (*Copy*)

   Penyalinan (*Copy*) merupakan fitur utama dari mesin fotokopi yaitu untuk menggandakan dokumen (*hard copy)* yang dicetak.

2. Pencetakan (Printing)

   Pencetakan (*Printing*) merupakan fitur yang melekat pada mesin fotokopi. Fitur ini berfungsi untuk mencetak dokumen (*soft copy)* langsung dari komputer pengguna yang telah terkoneksi dengan mesin fotokopi tersebut.

3. Kotak surat (*Mail box*)

   Mail box berfungsi untuk menyimpan data hasil pemindaian dokumen yang sering digandakan, ini dapat dilakukan karena mesin fotokopi jenis ini telah dilengkapi dengan perangkat *hard disk* mesin fotokopi maka hal ini memungkinkan beberapa data *scan* disimpan melalui fitur ini. Sehingga jika suatu saat dokumen tersebut akan dicetak kembali maka *user* bisa langsung mengambil data tersebut di penyimpanan *mail box. Mail box* mendukung berkas penyimpanan maksimal sebanyak 100 user.

4. Memindai (*Scan*)

   Fungsi memindai (*Scan*) difungsikan untuk mengubah file (gambar/tulisan) yang berbentuk *Hard copy* menjadi *Soft copy*, dapat berupa format TIFF atau PDF dan hasil scan tersebut dapat di simpan pada *mail box* maupun pada komputer yang telah terkoneksi dengan mesin fotokopi dan telah terinstal *Driver Scan Gear Tool.*

4.2 Implementasi Penelitian

Pada subbab ini akan dibahas mengenai implementasi penelitian yang merupakan hasil dari metode dan desain penelitian pada bab sebelumnya. Implementasi penelitian bertujuan untuk memastikan bahwa rumusan masalah dalam penelitian ini dapat terjawab.

Penelitian diawali dengan menghadirkan sebuah mesin fotokopi MFP merek Canon seri iR6000. Mesin fotokopi tersebut berada dalam kondisi baik dan layak beroperasi. Akuisisi objek penelitian tersebut diakuisisi dalam 2 (dua) kondisi penanganan, yaitu :

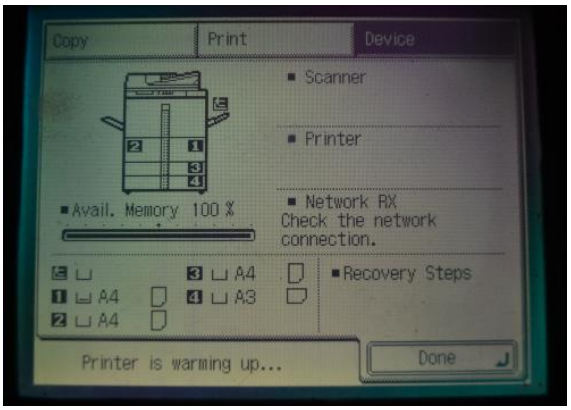
1. Perangkat dalam keadaan menyala (On).
2. Perangkat dalam keadaan padam (Off).

Implementasi ini dimaksud untuk mendapatkan gambaran lengkap dari kedua jenis tindakan akuisisi.

4.2.1 Teknik Akuisisi Langsung (*Live Aqcuisition)*

Diasumsikan perangkat mesin ditemukan dalam keadaan menyala. Beberapa tindakan yang dapat dilakukan seperti mendokumentasikan beberapa informasi terkait data yang dapat digunakan pada laporan teknis. Dokumentasi berupa pencatatan spesifikasi teknis mesin termasuk mencatat tanggal/waktu dari mesin fotokopi tersebut, fotografi forensik, serta pengecekan layanan antarmuka (*remote UI*) yang disediakan oleh Canon iR6000 melalui *web browser*, pada komputer yang telah terkoneksi dengan mesin.

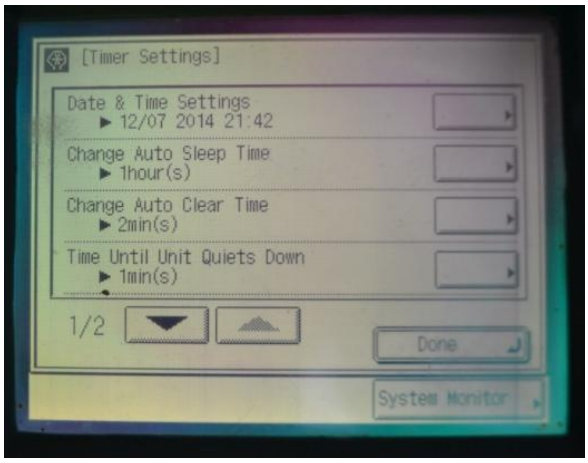
4.2.1.1 Akuisisi Pada Perangkat Canon iR 6000



Gambar 4. 1 Tampilan layar normal pada Touch Panel

1. Pengecekan waktu dan tanggal pada mesin.

   Pengecekan waktu dilakukan untuk mengetahui informasi terkait waktu dan tanggal yang telah diatur pada mesin fotokopi.



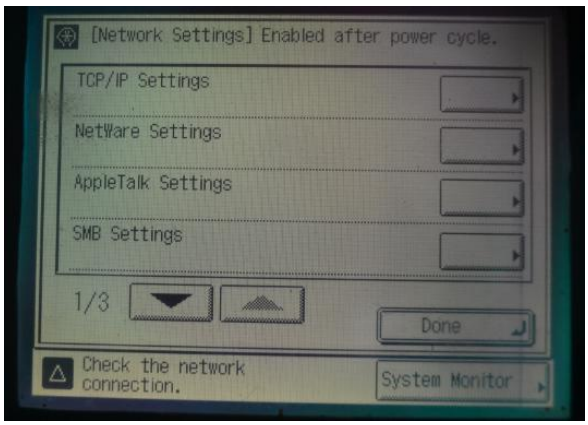
Gambar 4. 2 Tampilan *Timer Setting* pada *Touch Panel*

   Seperti yang terlihat pada gambar 4.2 tersebut seorang ahli forensik dapat melihat, mencatat dan melakukan pengambilan gambar guna mencocokkan waktu yang tertera pada mesin fotokopi dengan waktu menurut ahli forensik.

2. Pengecekan pengaturan jaringan

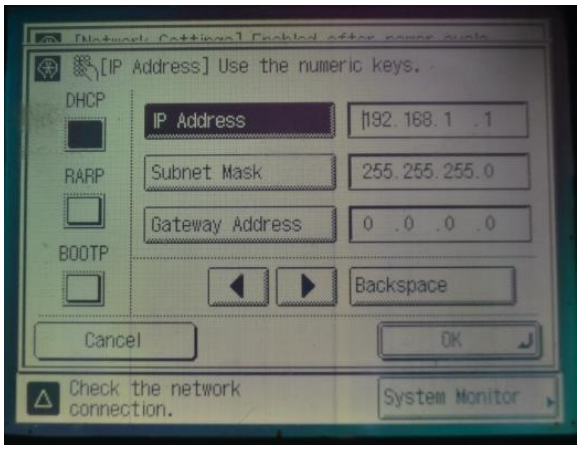
   Utilitas UI (*User Interface*) pada iR 6000, mentransformasi pengguna dengan layanan Desktop sebagai akses remote. Dengan memasukkan

alamat IP pada perangkat mesin fotokopi dan diakses dari *web browser* standar, pengguna dapat mengakses ke status perangkat dan pengaturan, fungsi *job-management* serta *mail box* tanpa tambahan perangkat keras atau lunak. Pengecekan pengaturan jaringan dilakukan guna mengetahui pengaturan jaringan yang dilakukan pada mesin fotokopi. Jaringan lokal pada mesin fotokopi dilakukan dengan sambungan kabel LAN (*Local Area Network*) untuk menghubungkan mesin fotokopi dengan perangkat lainnya seperti komputer.



Gambar 4. 3 Tampilan Network Settings pada Touch Panel

Seperti yang terlihat pada Gambar 4.3, beberapa fitur layanan pengaturan yang terdapat pada menu *Network Settings.* Untuk mengatur koneksi terhadap perangkat komputer, pengaturan dilakukan pada menu *TCP/IP Settings.*



Gambar 4. 4 Tampilan *IP Address* pada *Touch Panel*

Seperti yang terlihat pada gambar 4.4, pengaturan *IP Address* oleh pengguna mesin fotokopi yaitu:

IP Address : 192.168.1.1

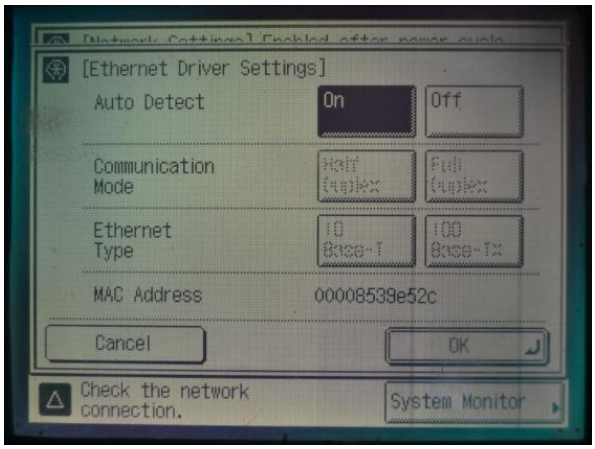
Subnet Mask : 255.255.255.0

Gateway Address: 0.0.0.0

Dengan data tersebut seorang ahli forensika digital dapat melihat, mencatat dan melakukan pengambilan gambar serta melakukan pengaturan jaringan langsung pada komputer ahli forensik, jika pemeriksaan langsung dibutuhkan.

3. Pengecekan MAC Address

Dalam sebuah jaringan berbasis Ethernet, *MAC Address* merupakan alamat yang unik yang memiliki panjang 48-bit (6byte) yang mengidentifikasi sebuah komputer, *interface* dalam sebuah *router* atau *node* lainnya dalam jaringan.

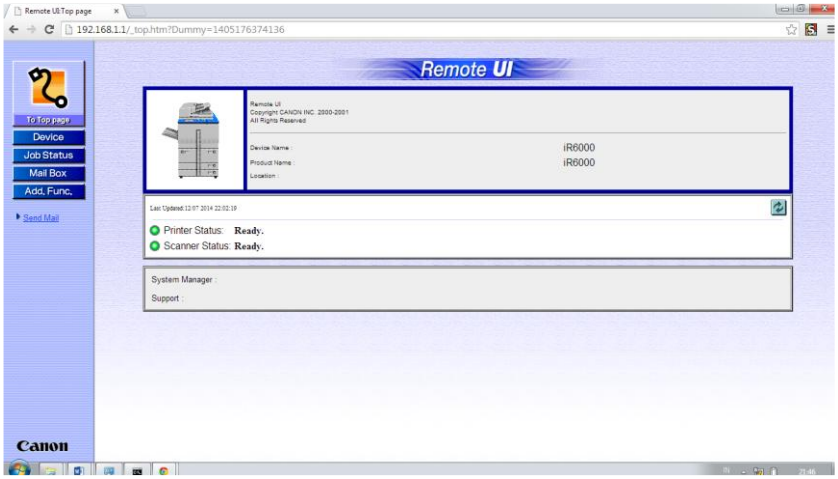


Gambar 4. 5 Tampilan *MAC Address* pada *Touch Panel*

Dapat dilihat *MAC Address* pada mesin fotokopi yang digunakan sebagai penelitian adalah ***00008539e52c.***

4.2.1.2 Akuisisi Memanfaat Layanan Remote UI Canon iR6000

Akuisisi menggunakan layanan *Remote UI* memanfaatkan koneksi perangkat mesin dengan komputer yang sebelumnya telah di konfigurasi. Utilitas UI (*User Interface*) pada iR6000 mentransformasi pengguna dengan layanan Desktop sebagai akses remote. Dengan me konfigurasi alamat IP pada perangkat mesin fotokopi dan diakses melalui web browser standar. Ahli forensika dapat mengakses ke status perangkat dan pengaturan, fungsi *job-management* serta *mail box* tanpa penambahan perangkat lunak.



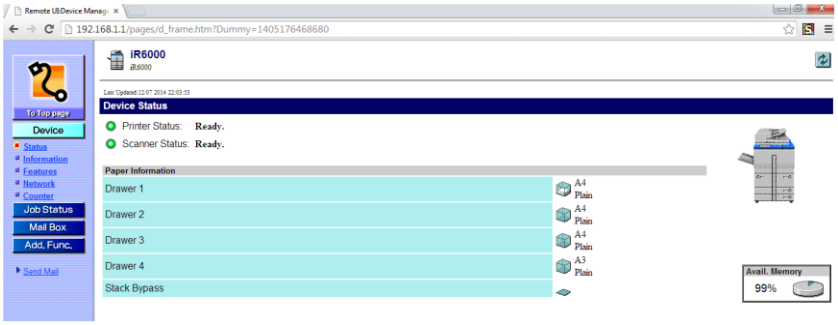
S

Gambar 4. 6 Tampilan *Remote UI*

Beberapa informasi yang di dapatkan melalui pemeriksaan *Utilitas UI* adalah sebagai berikut:

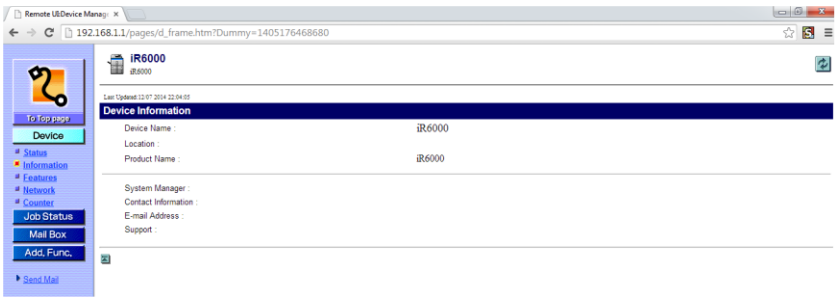
1. Device (Perangkat)

   Layanan informasi *device* (perangkat) meliputi informasi *Status* (Status mesin), *Information* (Informasi), *Features* (Fitur), *Network* (Jaringan), *Counter* (hitungan).



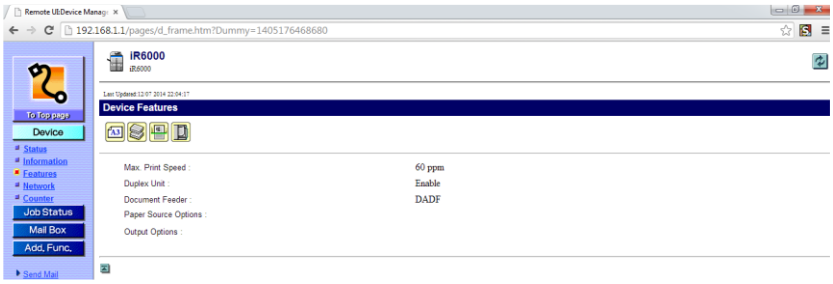
Gambar 4. 7 Tampilan *Status* pada *Remote UI*

Pada tampilan gambar 4.7, terlihat status layanan *printer* (pencetakan) dan *scanner* (pemindaian) dalam keadaan siap digunakan (*ready*).



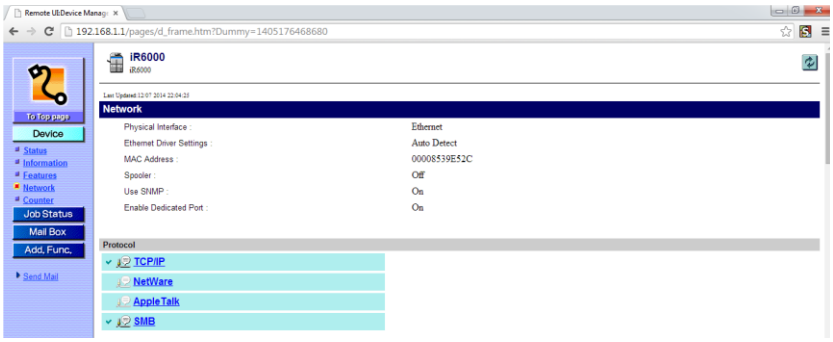
Gambar 4. 8 Tampilan *Device>Information* pada *Remote UI*

Pada gambar tampilan 4.8, terdapat informasi mengenai nama perangkat dan nama produk yang terekam pada sistem perangkat tersebut. Ini digunakan jika adanya usaha kamuflase dari bentuk perangkat secara visual.



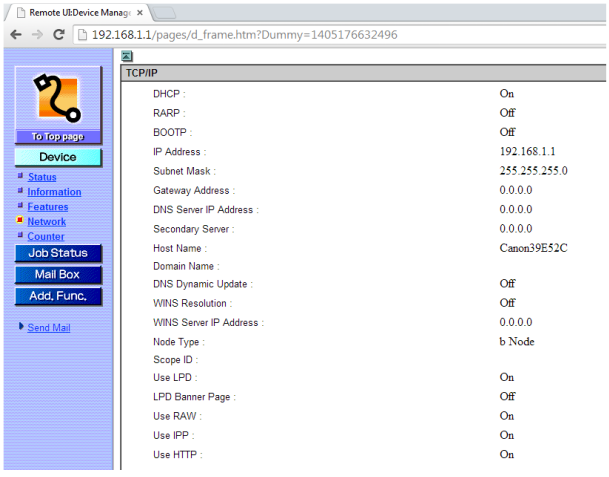
Gambar 4. 9 Tampilan *Device>Features* pada *Remote UI*

Pada gambar tampilan 4.9, terdapat informasi fitur-fitur dari mesin Canon iR6000, seperti kecepatan cetak yang mencapai 60 ppm.



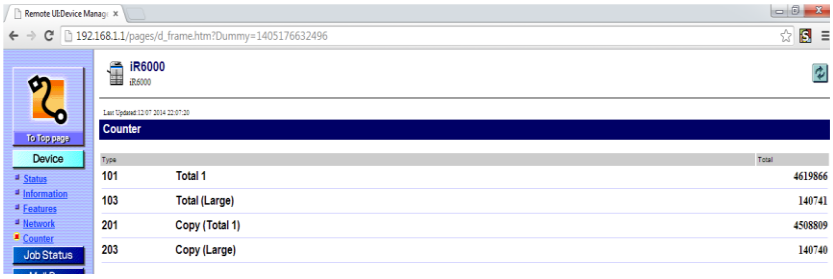
Gambar 4. 10 Tampilan *Device>Network* pada *Remote UI*

Pada gambar tampilan 4.10, terdapat informasi mengenai jaringan, *Mac Address* dan beberapa protokol seperti TCP/IP, NetWare, AppleTalk dan SMB.



Gambar 4. 11 Tampilan *Network TCP/IP* pada *Remote UI*

Pada tampilan gambar 4.11 terdapat informasi detail dari jaringan TCP/IP yang di gunakan oleh mesin. Dari tampilan tersebut dapat diketahui bahwa informasi pengaturan alamat IP saat akuisisi langsung pada mesin adalah sama.

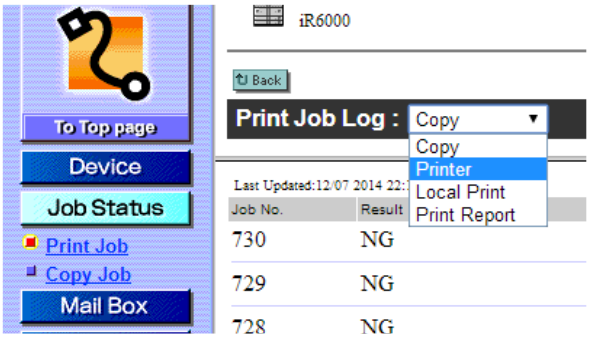


Gambar 4. 12 Tampilan *Counter* pada *Remote UI*

Pada tampilan gambar 4.12, terdapat detail informasi jumlah pencetakan yang pernah dilakukan oleh perangkat mesin fotokopi tersebut.

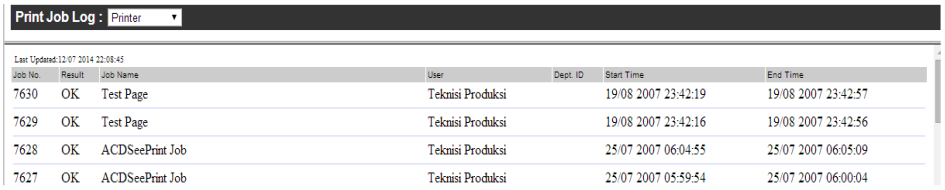
2. Job Status (Status Pekerjaan)

Layanan *job status* menyimpan informasi yang diperlukan untuk mengetahui pekerjaan apa saja yang telah dikerjakan oleh mesin. Layanan *job status* meliputi informasi historis pekerjaan mencetak (*print Job*) dan menyalin (*Copy job*). Pada layanan *Print Job* terdapat 4 kategori *log* yaitu *Copy, Printer, Local Print, Print Report.*



Gambar 4. 13 Tampilan *Job Status* pada *Print Job* pada *Remote UI*

Tampilan tabel *print Job log* menyediakan beberapa informasi seperti nomor bilangan pekerjaan (*Job No*), keterangan Hasil (*result*), Keterangan Pengguna (*User*), Identitas Kelompok (*Dept Id*), Waktu Mulai (*Start Time*) dan waktu selesai (*End Time*). Hal ini juga berlaku pada *Print job log* untuk informasi *Copy, Local Print, Print Report.*

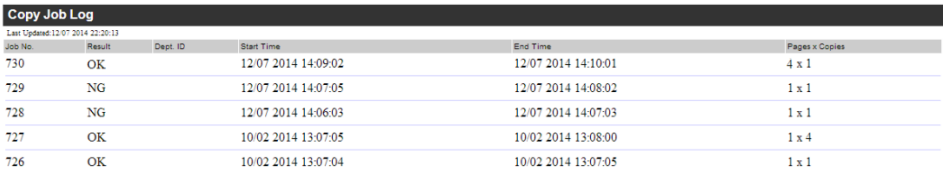

Print Job Log : Printer

Last Updated:12/07 2014 22:08:45

Job No.	Result	Job Name	User	Dept. ID	Start Time	End Time
7630	OK	Test Page	Teknisi Produksi		19/08 2007 23:42:19	19/08 2007 23:42:57
7629	OK	Test Page	Teknisi Produksi		19/08 2007 23:42:16	19/08 2007 23:42:56
7628	OK	ACDSeePrint Job	Teknisi Produksi		25/07 2007 06:04:55	25/07 2007 06:05:09
7627	OK	ACDSeePrint Job	Teknisi Produksi		25/07 2007 05:59:54	25/07 2007 06:00:04

Gambar 4. 14 Tampilan keterangan *log* informasi pada *Print Job log*

Tabel *copy job log* menyediakan informasi yang berbeda dari *print job log.* Pada informasi *copy job log* menyediakan informasi tambahan yaitu jumlah lembar kertas yang disalin dalam sekali instruksi penyalinan (*page x copies*),


Copy Job Log

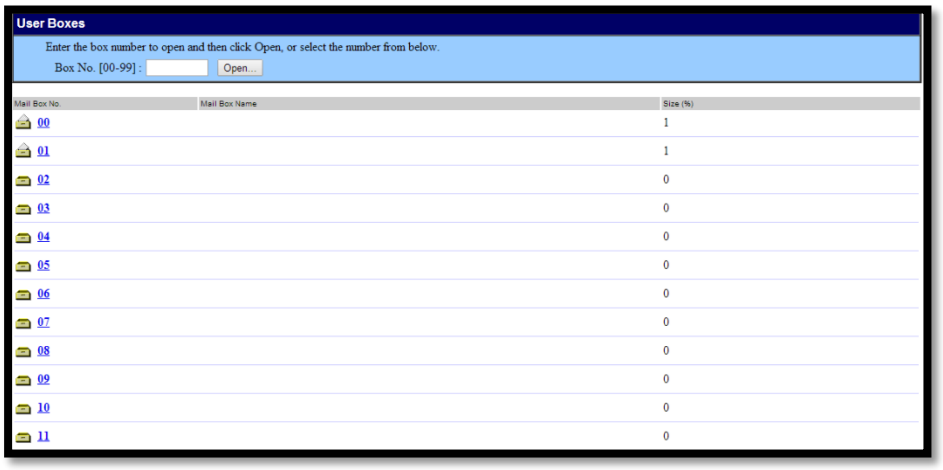
Last Updated:12/07 2014 22:20:13

Job No.	Result	Dept. ID	Start Time	End Time	Pages x Copies
730	OK		12/07 2014 14:09:02	12/07 2014 14:10:01	4 x 1
729	NG		12/07 2014 14:07:05	12/07 2014 14:08:02	1 x 1
728	NG		12/07 2014 14:06:03	12/07 2014 14:07:03	1 x 1
727	OK		10/02 2014 13:07:05	10/02 2014 13:08:00	1 x 4
726	OK		10/02 2014 13:07:04	10/02 2014 13:07:05	1 x 1

Gambar 4. 15 Tampilan keterangan *log* informasi pada *Copy Job log*

3. *Mail box* (Kotak penyimpanan)

Mail box berfungsi sebagai tempat menyimpan data hasil *scan* dokumen. Penyimpanan hasil pindai di *mail box* merupakan aksi yang disengaja oleh pengguna. *Mail box* terdiri dari *folder-folder* atau kontak penyimpanan yang dapat diatur untuk memisahkan penempatan data yang disimpan.



Gambar 4. 16Tampilan *mail box* pada *Remote UI*

Melalui layanan *remote UI* file tersebut dapat diambil untuk dilakukan pemeriksaan oleh ahli forensik. File tersebut ditemukan berekstensi (*.jbg*) menurut format tersebut, file yang ditemukan termasuk kategori file gambar.

4.2.2 Teknik Akuisisi Diam (*Static Aquisition)*

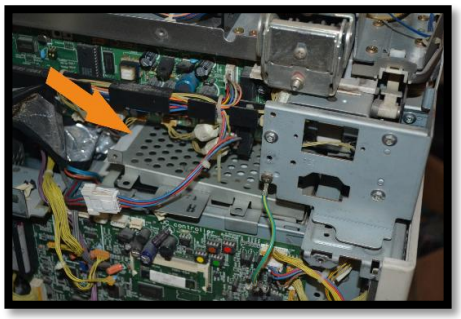
Mesin telah dipastikan padam dengan pengecekan kabel Power yang tersambung pada arus listrik. Setelah melakukan dokumentasi (Foto forensik dan Pencatatan) pada perangkat, maka tahap selanjutnya adalah mengakuisisi media penyimpanan *non-volatile (hard disk)* guna mengetahui artifak-artifak yang tersimpan. Beberapa tahapan umum yang dilakukan pada pemeriksaan objek penelitian dalam keadaan padam adalah sebagai berikut:

1. Memastikan mesin tersebut dalam keadaan mati dengan mengecek kabel arus listrik.
2. Mencatat spesifikasi dari mesin mencakup *serial number*, merek dan jenis.
3. Lakukan fotografi forensik terhadap mesin.
4. Mengambil/memisahkan media penyimpanan *non-volatile* (*hard disk*) dari perangkat mesin fotokopi MFP.
5. Melakukan prosedur dan tahapan akuisisi.

4.2.2.1 Akuisisi Pada Penyimpanan Non-volatile

Hard disk tersimpan di dalam perangkat mesin fotokopi yang hanya bisa diakses/diambil dengan cara membuka cover belakang pada perangkat (Gambar 4.19). Seperti di tunjukan oleh panah berwarna oranye pada Gambar 4.20 tersebut merupakan letak posisi *Hard disk* yang terdapat setelah sampul belakang mesin dibuka. Media penyimpanan *non-volatile* (*Hard disk*) pada perangkat penelitian memiliki informasi keterangan, sebagai berikut :

Gambar 4. 17 Tampilan kerja pembukaan cover belakang



Gambar 4. 18 Tampilan lokasi peletakan *Hard disk* pada iR6000

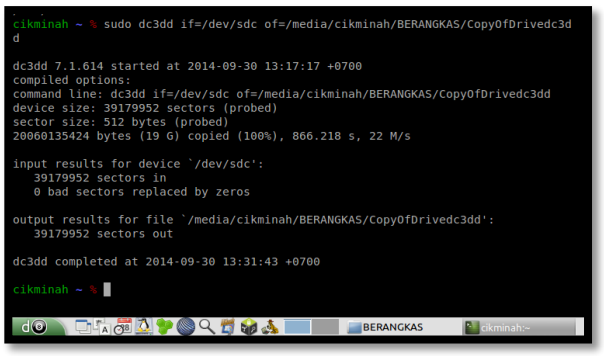
Gambar 4. 19 Tampilan Penyimpanan non-volatile (*Hard disk*)

Keterangan *Hard disk*:

- Merek : Samsung
- Serial Number : 0442J1FT809832
- Kapasitas : 20 GB
- Tipe Hard disk : ATA (IDE)

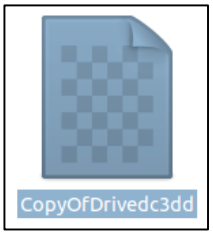
4.2.2.2 *Hard Drive Imaging*

Imaging pada media penyimpanan dilakukan penyalinan *bit stream copy*. Teknik *imaging* yang digunakan adalah "*Bit-stream disk-to-image file. Imaging* di lakukan dengan bantuan perangkat lunak DC3DD yang berjalan pada sistem operasi DEFT versi 8.2 . Serta menggandakan isi hasil *imaging* sebagai salah satu prosedur penanganan barang bukti elektronik.



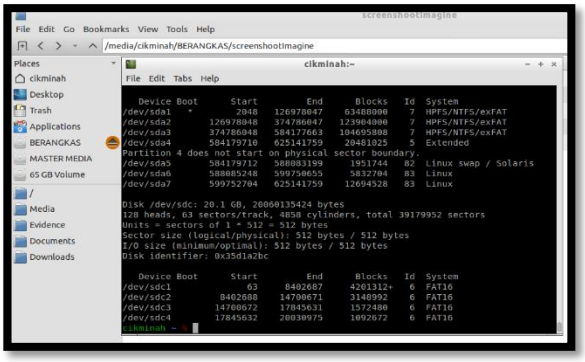
Gambar 4. 20 Tampilan *forensik imaging* dengan bantuan DC3DD

Hasil *Imaging*, menghasilkan file berformat *".dd"*. Peneliti menamai file hasil dengan *"CopyOfDrivedc3dd"*.



Gambar 4. 21 File hasil *imaging* dengan bantuan DC3DD

Sebelum *forensik imaging* dilakukan, prosedur *write protect* dilakukan. *Write Protection* merupakan salah satu teknik awal untuk menjaga barang bukti orisinal dari perubahan-perubahan yang tidak disengaja dilakukan oleh ahli forensik. Deft mengakomodasi setiap perangkat penyimpanan baru yang terdeteksi secara *default* tidak dapat di tulis dan diakses.

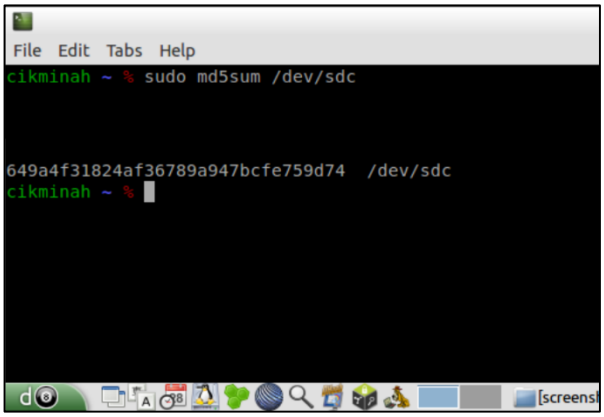


Gambar 4. 22 Konsep *write protection* pada Sistem Operasi Deft

Pada gambar 4.22 (Tampilan terminal) di atas perangkat dideteksi sebagai "`Disk /dev/sdc:20.1 GB, 20060135424 bytes`" sedangkan pada tampilan *Desktop*, drive itidak di tampilkan.

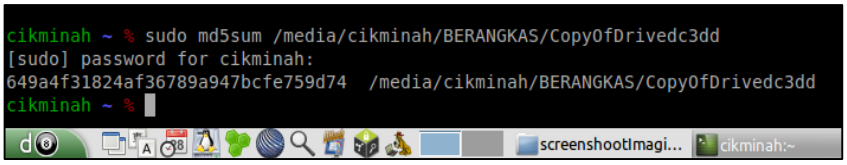
4.2.2.3 *Hard Drive Hashing*

Proses *hashing* dilakukan dilakukan pada dua buah kondisi pengukuran, yaitu pada *hard disk* sumber saat sebelum dilakukan *forensik imaging* dan setelah proses *imaging* yang dilakukan pada file hasil *imaging*.



Gambar 4. 23 Tampilan *hasing* MD5 pada *hard disk* sumber

Hasil *hasing* MD5 pada *hard disk* sumber menunjukkan nilai *"649a4f31824af36789a947bcfe759d74 /dev/sdc"*

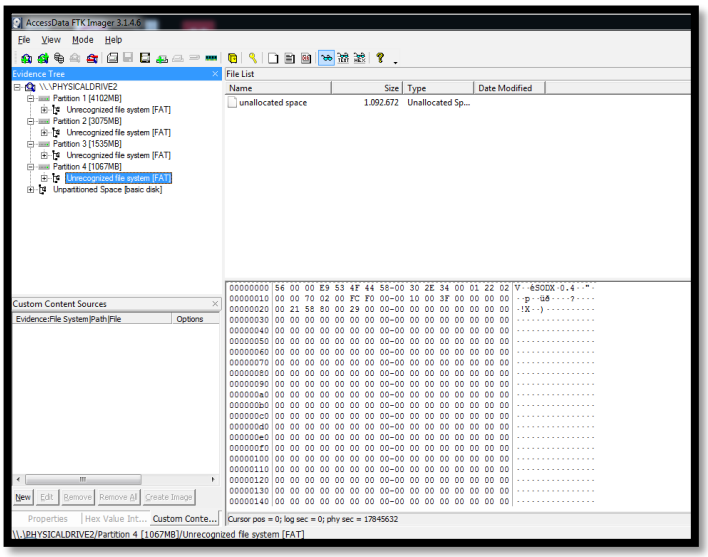


Gambar 4. 24 *hasing* MD5 pada *image file* hasil *forensik imaging*

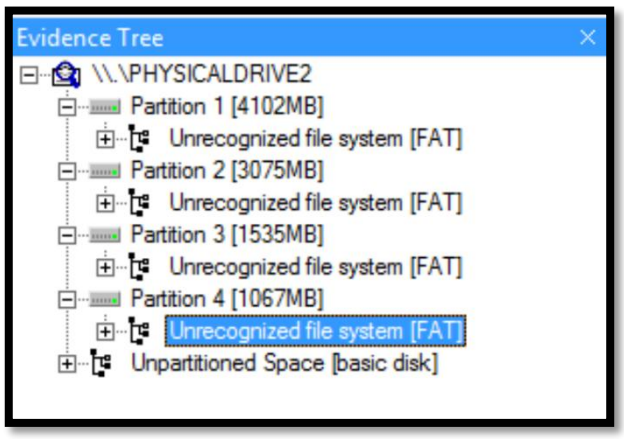
Hasil *hasing* MD5 pada *image file* hasil *forensik imaging* menunjukkan nilai *"649a4f31824af36789a947bcfe759d74"/../CopyOfDriveddc3dd.* Merunut dari nilai *hashing* yang sama antara file sumber dan *image file* dari hasil *forensik imaging* maka *image file* dinyatakan otentik dan dapat dilakukan ke tahap penyelidikan selanjutnya.

4.2.2.4 Ekstraksi dan Analisis *Image File*

Ekstraksi data dan analisis merupakan tahapan yang dilakukan setelah tahap *forensik imaging* selesai dilaksanakan. Tahapan ini dilakukan dengan menggunakan *tool forensik analysis* yang sama, dikarenakan *software* dipakai dapat mengakomodasi kedua tahapan tersebut.



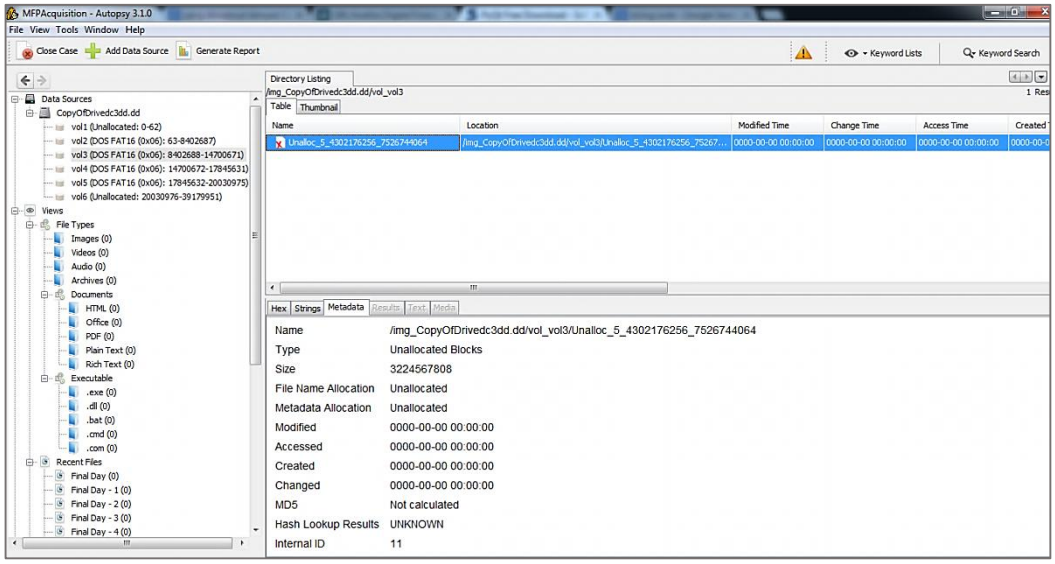
Gambar 4. 25 Tampilan ekstraksi dan analisis dengan AccessData FTK *Imager*



Gambar 4. 26 Tampilan *file image* yang diekstrak

Gambar 4.26 ditampilkan bahwa *hard disk* objek penelitian memiliki 4 buah partisi yang memiliki kapasitas berbeda-beda dengan *file system* FAT. Namun *tool forensik analysis* FTK *Imager* tidak dapat membaca atau mendukung pembacaan *file system* dari *hard disk* objek penelitian tersebut (*Unrecognized file system*). File List FTK *Imager* menampilkan "*unallocated space"*pada setiap partisi yang diaktifkan untuk dianalisis sehingga disimpulkan penggunaan *tool forensik analysis* FTK *Imager* tidak dapat digunakan dalam menganalisis penelitian ini.

Peneliti melanjutkan proses analisis dengan menggunakan *tool forensik analysis Autopsy 3.1.0.*



Gambar 4. 27 Tampilan ekstraksi dan analisis dengan Autopsy

Proses ekstraksi pada Autopsy berjalan lancar, *drive image* dibagi menjadi 6 (enam) buah partisi yang tidak memiliki kemampuan pembaca file system pada Autopsy.

CODE	TYPE	STARTING SECTOR	LENGTH IN SECTOR	SIZE (Byte)
Vol 1	Unallocated Blocks	0	62	32256
Vol 2	DOS FAT 16 (0x06)	63	8402687	4302144000
Vol 3	DOS FAT 16 (0x06)	8402688	14700671	3224567808
Vol 4	DOS FAT 16 (0x06)	14700672	17845631	1610219520
Vol 5	DOS FAT 16 (0x06)	17845632	20030975	1118896128
Vol 6	Unallocated Blocks	20030976	39179951	9804275712

Tabel 4.1 Keterangan Boot Volume Header pada proses ekstraksi Autopsy

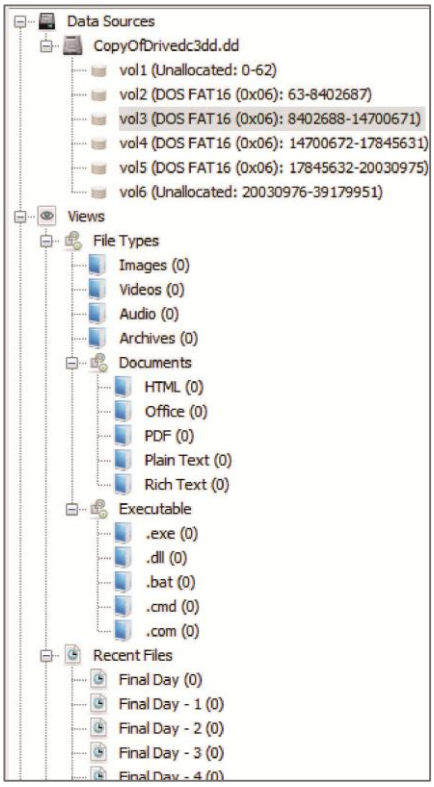
Enam partisi memiliki *boot volume header* sebagai berikut:

1. **V...SODX.0.4.....p.......?..... ..)**
2. **adaNF_sFVtsaTltcelba..**
3. **V...SODX.0.4..a...p.......?.....`...)**
4. **V...SODX.0.4..a...p.......?.....`...)**
5. **V...SODX.0.4.."...p.......?.....!X..)**
6. ***(offset 0-16.384 contains no text)***

"SODX" dapat ditafsirkan sebagai inisial dari nama sebuah *file system.* Namun bagaimanapun *filesystem* tersebut tidak dapat dikenali.

Proses analisis pada *drive* DOS FAT 16 tidak dapat dilakukan dikarenakan *Directory Listing* pada Autopsy menunjukkan *"analloc_5..."* yang artinya Drive dianggap tidak terisi (Gambar 4.28) Hasil *view* berbagai tipe file (*image, video, audio, Archive*), Dokumen (*HTML, Office, PDF, Plain text, Rich text*) dan file *excuteable* juga ditandai dengan nilai "0" (kosong).

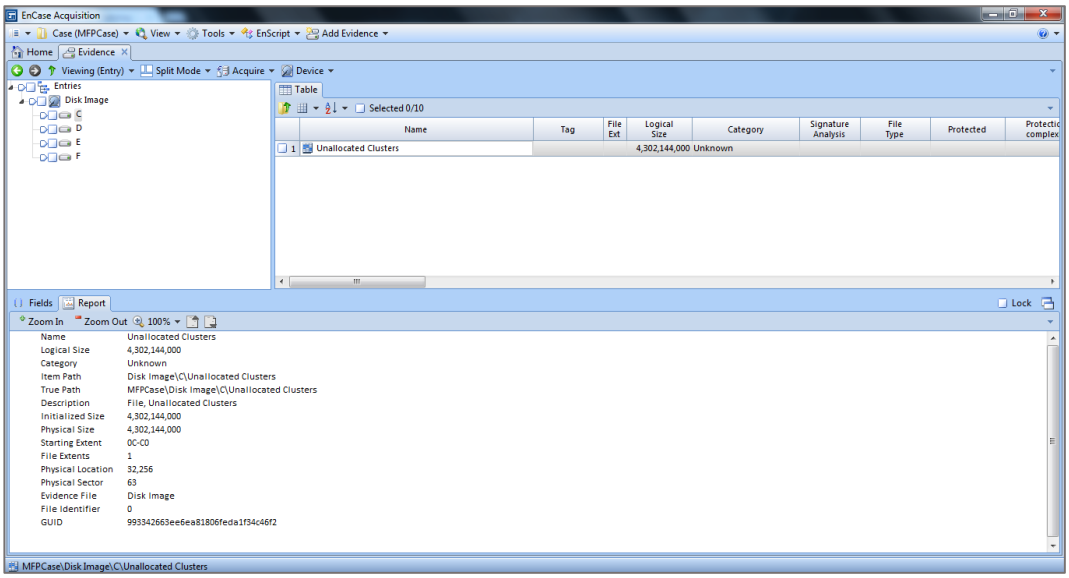
Sehingga disimpulkan penggunaan *tool forensik analysis* Autopsy tidak dapat digunakan dalam menganalisis penelitian ini



Gambar 4. 28 Tampilan *Tree Table* Ekstraksi dan *file view Autopsy*

Gambar 4. 29 Tampilan *Directory Listing* pada Autopsy

Peneliti melanjutkan proses analisis dengan menggunakan *tool forensik analysis EnCase.* Proses ekstraksi menggunakan EnCase berjalan lancar dan menampilkan 4 buah partisi yang berhasil di ekstrak. Proses analisis tidak dapat dilakukan, karna Encase tidak dapat mengenali sistem file (*Unallocated Clusters*) dari setiap partisi yang diekstrak. Sehingga disimpulkan penggunaan *tool forensik analysis EnCase* tidak dapat digunakan dalam menganalisis penelitian ini



Gambar 4. 30 Tampilan ekstraksi dan analisis dengan EnCase Acquistion

4.3 Hasil dan Pembahasan Implementasi Penelitian

Implementasi penelitian menemukan beberapa temuan antara lain:

1. Kedua teknik forensika digital (*live acquisition* dan *static acquisition*) dapat dilakukan dalam pemeriksaan forensika digital mesin fotokopi.
2. Teknik *live Acquisition* forensika digital berhasil menemukan sebagian besar informasi terkait perangkat mesin fotokopi baik baik info hardware maupun konfigurasinya. Teknik forensika digital juga mampu menemukan informasi historis pekerjaan mencetak (*print Job*) dan menyalin (*Copy job*). Historis tersebut terbagi kedalam 4 (empat) kategori *log* yaitu *Copy*, *Printer*, *Local Print*, *Print Report.* Selain itu, pada usaha penyalinan dokumen, ahli forensik juga mendapatkan informasi jumlah lembar kertas yang disalin dalam sekali intruksi penyalinan (*page x copies*). Secara keseluruhan artifak yang didapat dari mesin fotokopi adalah :
   - Nomor bilangan pekerjaan (*Job No*),
   - Keterangan Hasil (*result*),
   - Keterangan Pengguna (*User*),

- Identitas Kelompok (*Dept Id*),
- Waktu Mulai (*Start Time*) dan
- waktu selesai (*End Time*).
- Jumlah kertas yang disalin dalam sekali penyalinan (*page x copies)*

3. Pemeriksaan *mail box* pada layanan *remote UI* menghasilkan temuan file-file dokumen yang disimpan sebagai data *non-volatile* di mesin fotokopi. File tersebut merupakan hasil sebuah aksi dari tindakan perekaman yang disengaja oleh operator mesin fotokopi. file yang ditemukan berekstensi " *".jbg"* yaitu suatu bentuk file dengan tipe komprensi gambar (*lossless*). File ini dapat ditampilkan dengan bantuan prangkat lunak ke-3 seperti *XnView*.
4. Teknik *static acquisition* dianggap tidak dapat dilakukan dalam memforensik perangkat mesin fotokopi MFP. Kendala yang dialami adalah belum adanya *tool forensik analysis* yang peneliti dapati dan gunakan untuk mengekstraksi dan mengenali file data saat melakukan proses analisis pada barang bukti *hard disk.*
5. Jika mesin fotokopi berada dalam kondisi padam pada saat penyelidikian seorang ahli forensik harus tetap mengambil langkah *live acquisition* dengan cara menyalakan mesin fotokopi kembali.
6. Akuisisi *live acquisition* dilakukan pada perangkat mesin dan komputer dengan memanfaatkan layanan *remote UI.*

4.4 Perancangan Kerangka Kerja Investigasi Forensika Digital pada Mesin Fotokopi MFP

Belum adanya *tool forensik analysis* yang mampu melakukan investigasi secara *static acquisition,* memaksa seorang ahli forensika digital harus mampu melakukan *live acquisition* di TKP pada barang bukti mesin fotokopi yang ditemukan.

Adapun kerangka kerja investigasi forensika digital pada mesin fotokopi MFP secara umum dibuat berdasarkan perpaduan dua buah bentuk pemodelan yaitu model proses investigasi *carrier* yang membedakan teknis investigasi forensika digital *Phisical* dan *virtual* serta kerangka kerja *Electronic Discovery Reference Model* (EDRM).

Model investigasi Carrier secara eksplisit menggambarkan hubungan secara paralel antara proses penanganan Tempat Kejadian Perkara (TKP) dan penanganan barang bukti digital. Pada waktu yang sama juga dapat terlihat bahwa perbedaan yang signifikan dari kedua proses penanganan investigasi tersebut.

Table 6.1 Phases of Digital and Physical Investigations in Carrier's Integrated Digital Investigation Process Model

	Phase Goals (Physical)	Phase Goals (Digital)
Crime scene preservation	Securing entrances and exits and preventing physical changes to evidence	Preventing changes in potential digital evidence, including network isolation, collecting volatile data, and copying entire digital environment
Crime scene survey	Walking through scene, identifying obvious and fragile physical evidence	Identification of obvious evidence by searching in digital evidence (typically in lab)
Crime scene documentation	Photographs, sketches, maps of evidence, and crime scene	Photographs of digital devices and individuated descriptions of digital devices
Crime scene search and collection	In-depth search for physical evidence	Analysis of system for nonobvious evidence (typically in lab)
Crime scene reconstruction	Developing theories based on analysis results and testing against evidence	

Gambar 4. 31 Tahapan Proses Investigasi digital Carrier's

Perpaduan kedua model investigasi dilakukan karena mengingat mesin fotokopi MFP memiliki karakter barang bukti elektronik yang unik. Mesin Fotokopi MFP dapat membentuk artifak tidak hanya berbentuk berkas elektronik namun juga dapat menciptakan artifak berbentuk benda (Hasil cetakan) yang memungkinkan dijumpai oleh investigator saat pemeriksaan atau penanganan kasus terkait perangkat ini.

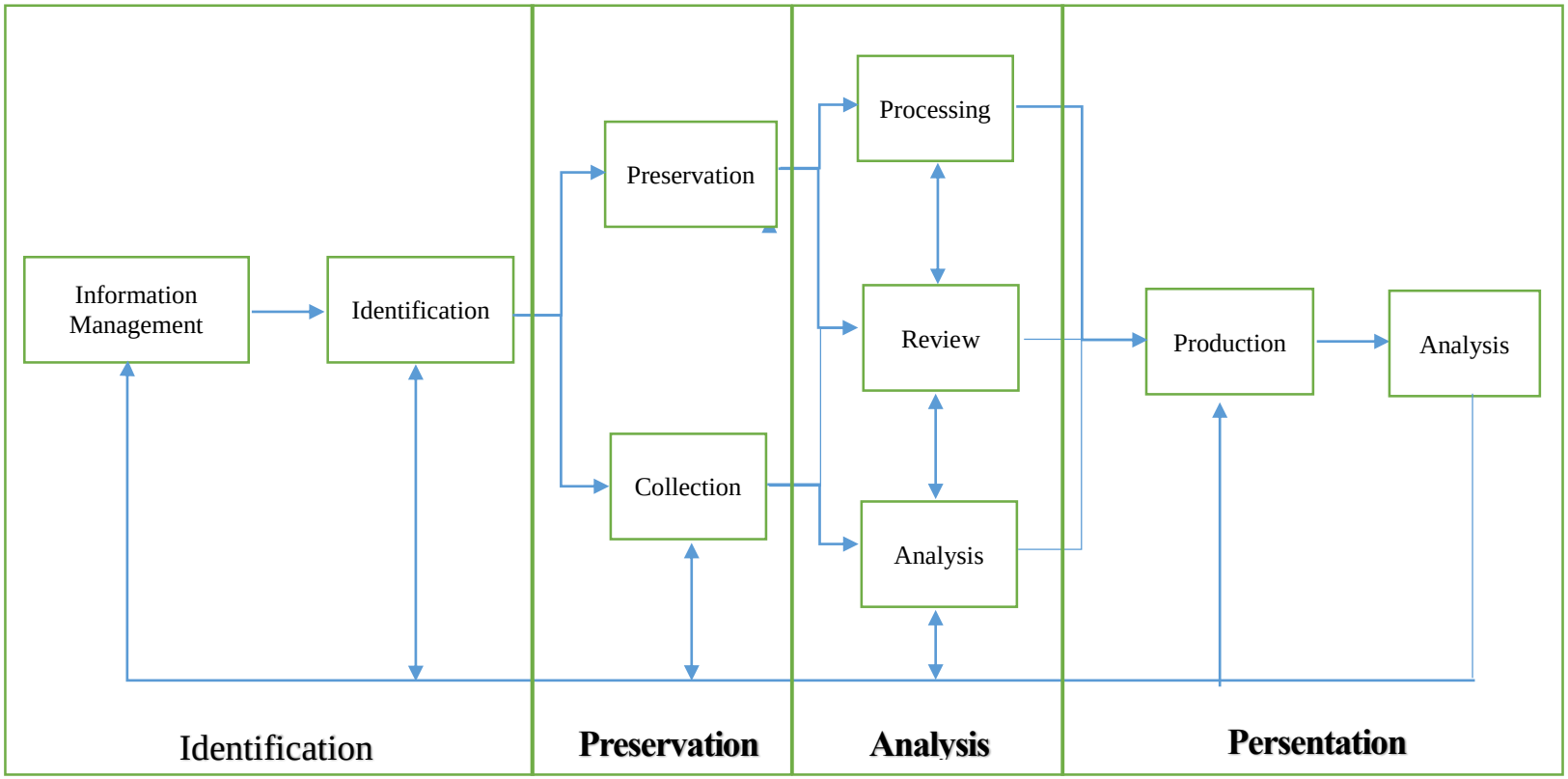
Kerangka kerja *Electronic Discovery Reference Model* (EDRM) merupakan pemodelan utama yang digunakan dalam perancangan kerangka kerja investigasi forensika digital pada mesin fotokopi MFP. Namun dilakukan penyesuaian dengan mengubah beberapa fitur seperti fitur seperti tahapan *Review*

pada blok *Analysis.* Tahapan Review pada EDRM berfungsi sebagai letigasi dan digunakan untuk mengidentifikasi dokumen tindakan responsif seperti penahanan pelaku. Penahanan yang dimaksud yaitu di saat tim tim hukum (pengadilan) mendapatkan pemahaman lebih lanjut dari masalah faktual secara dokumen pada kasus yang dihadapi. Pada tahap ini akan membahas banyak faktor yang harus dipertimbangkan dalam mempersiapkan dokumen dan mengelolanya sampai selesai sehingga disimpulkan pengambilan tindakan responsif tidak dapat diambil saat di TKP (Edrm.net, 2005).

Pada konteks penanganan mesin forensika digital mesin fotokopi MFP yang dilakukan secara *live Acquisition* maka tahapan pengambilan tindakan responsif belum dapat dilakukan karena proses investigasi dilaksanakan secara langsung di TKP. Oleh sebab itu tahapan *review* pada blok *Analysis* ditiadakan pada perancangan kerangka kerja investigasi forensika digital pada mesin fotokopi MFP.

KERANGKA KERJA

ELECTRONIC DISCOVERY REFERENCD MODEL (EDRM)



Gambar 4. 32 *Electronic Discovery Reference Model* (EDRM) *Schema*

Electronic Discovery Reference Model (EDRM) diadopsi guna merancang kerangka kerja investigasi forensika digital pada mesin fotokopi MFP. EDRM hasil penyesuaian dibagi ke dalam empat bagian yang dapat dijabarkan sebagai berikut:

A. Identifikasi

1. Manajemen Barang Bukti

   Manajemen barang bukti meliputi persiapan umum terhadap hal-hal seperti aturan tindakan (investigasi, pengledahan, penyitaan, penangkapan dan lain-lain), sumber daya dari penyidik yang diikutsertakan, Standar operasi yang diterapkan serta peralatan sebelum berangkat ke TKP untuk melaksanakan penanganan kasus yang berkaitan dengan barang bukti elektronik, seperti

   a. Administrasi investigasi: seperti surat perintah pengledahan dan surat perintah penyitaan.
   b. Alat – alat dokumentasi : Kamera dan alat tulis guna memotret barang bukti dengan teknik forensik dan mencatat spesifikasi teknis barang bukti yang ditemukan di TKP.
   c. Nomor, skala ukur, label lembaga, serta stiker, kantong plastik dan label kosong guna menandai masing-masing barang bukti elektronik yang ditemukan di TKP.
   d. *Triage tool :*digunakan untuk kegiatan *triage forensic* terhadap barang bukti mesin fotokopi yang ditemukan.

2. Identifikasi

   Identifikasi investigasi meliputi

   a. Pengolahan tempat kejadian perkara

      Adapun tahapan kerja dalam melakukan pengolahan tempat kejadian perkara dilakukan dengan tindakan-tindakan sebagai berikut

      - Pengamatan umum

        Pengamatan umum yakni pengamatan yang diarahkan terhadap hal-hal/obyek-obyek sebagai berikut:

        - Lokasi tempat keberadaan mesin fotokopi

- Model, jenis dan jumlah barang bukti
- Alat-alat pendukung yang digunakan/ditinggalkan si pelaku
- Bekas / jejak (hasil cetak) yang terdapat di sekitar mesin fotokopi
- Kondisi objek (mesin masih beroperasi/tidak)

Hasil dari pengamatan tersebut di atas dimaksudkan untuk dapat memperkirakan dengan cepat mesin fotokopi yang digunakan dalam operandi tersebut serta langkah-langkah mana yang terlebih dahulu dilakukan

b. Dokumentasi Barang Bukti

Dokumentasi yaitu Pemotretan dan pencatatan yang dilakukan dengan maksud untuk:

- Mengabadikan situasi TKP dan barang bukti pada saat ditemukan
- Memberikan gambaran nyata situasi barang bukti dan TKP
- Membantu dan melengkapi kekurangan dalam pengolahan TKP termasuk dalam pencatatan dan pembuatan laporan.

Objek pemotretan adalah:

- Objek kejadian perkara secara keseluruhan dari berbagai sudut
- Detail/*Close Up* terhadap barang bukti (mesin fotokopi) digunakan skala/ penggaris/ jam tangan ahli (dapat digunakan bersamaan dengan penanganan barang bukti)

Setiap pengambilan informasi dengan pemotretan maka ahli forensik harus membuat catatan sebagai penjelasan hasil pemotretan memuat:

- Hari, tanggal, bulan, tahun dan jam pemotretan
- Merek tipe kamera, lensa, dan film
- Kecepatan kamera dan diafragmanya

- Sumber cahaya
- Filter yang digunakan
- Jarak kamera terhadap objek (mesin fotokopi)
- Nama, pangkat, Nomor induk petugas yang melakukan pemotretan tersebut.

c. Dokumentasi Proses / Kegiatan Penyelidikan

Dokumentasi kegiatan penyelidikan mesti dilakukan baik secara tulis (berita acara/surat keterangan), fotografi (gambar) dan video.

d. Identifikasi Sumber daya

Identifikasi sumber daya dapat dibagi ke dalam dua jenis yaitu sumber daya manusia dan sumber daya perangkat yang ditemukan.

B. Pelestarian

1. Pelestarian Barang Bukti

a. Penanganan awal TKP

- Mengamankan lingkungan barang bukti. Barang bukti diamankan dari adanya kemungkinan usaha-usaha gangguan, pengrusakkan, penghilangan serta perubahan dari pihak luar. Oleh karena itu barang bukti sebaiknya dijaga selama proses akuisisi. Memberi garis pembatas (garis polisi) dan selanjutnya barang bukti di segel.
- Pengecekan koneksi mesin dengan perangkat lain

Catatan Penting:

Jika terdapat adanya koneksi kabel jaringan pada Port jaringan di mesin fotokopi, ahli forensik wajib langsung mencabut kabel jaringan tersebut. Agar tidak adanya usaha penghilangan data secara remote.

2. Pengumpulan Barang Bukti

Pengumpulan barang bukti merupakan tindakan mengumpulkan seluruh informasi dari perangkat fisik dan digital. Pengumpulan barang bukti secara fisik seperti:

a. Mencatat spesifikasi teknis dari perangkat / barang bukti yang ditemukan.
b. Mencatat keterangan saksi-saksi, pelaku, penyidik serta mendokumentasi dengan prinsip fotografi forensik
c. Menemukan jejak / artifak dari hasil cetakan dari lingkungan TKP. Jejak dapat berupa hasil cetakan rusak atau yang tidak digunakan.
d. Menemukan benda atau perangkat lain yang terhubung dengan perangkat barang bukti.

Pengumpulan barang bukti secara digital, seperti:

a. Mendokumentasi (foto forensik dan catat) segala informasi yang terdapat pada layar perangkat (kondisi menyala/on)
b. Informasi utama yang diambil yaitu waktu dan tanggal yang dikonfigurasi, no MAC mesin, konfigurasi IP (Networks), *mail box*.
c. Lakukan *Triage forensic*

C. Akuisisi

1. Akuisisi Bukti Digital

Adapun tahapan kerja akuisisi adalah sebagai berikut:

a. Pencarian bukti digital pada perangkat mesin fotokopi dilakukan pada kondisi mesin menyala / *live acquisition.*
b. Jika kondisi mesin padam maka ahli dapat meminta operator/tersangka untuk menyalakan kembali dengan pengawasan dan perhatian ketat dari investigator dan ahli forensik.

c. Jika tahapan penyalaan kembali oleh operator/tersangka dilakukan maka harus dibuat BAP dan dokumentasi saat proses berlangsung.
d. Jika tidak ditemukan operator dan tersangka maka ahli forensik dapat menghidupkan dengan video dokumentasi yang jelas dari setiap tahap penyalaan.
e. Pengumpulan informasi pada perangkat mesin fotokopi.
   - Pengumpulan informasi pada perangkat dilakukan dengan pemotretan dan pencatatan pada layar mesin fotokopi.
   - Informasi utama yang diambil yaitu waktu dan tanggal yang dikonfigurasi, no MAC mesin, konfigurasi IP (network), *mail box*.
f. Melakukan koneksi antara perangkat mesin dengan komputer / leptop ahli forensik.
g. Pengumpulan informasi perangkat mesin fotokopi dengan layanan *remote UI.*
   - Melakukan koneksi antara perangkat mesin dengan komputer ahli forensik.
   - Perangkat komputer atau leptop ahli dipastikan sesuai persyaratan sebagai perangkat investigasi.
   - Koneksi menggunakan kabel UTP RJ45
   - Konfigurasi jaringan LAN dengan pengaturan IP pada Komputer ahli forensik.
   - Pengaturan IP Komputer Ahli mesti bersumber dari pengaturan IP pada perangkat mesin fotokopi.
   - Setelah dipastikan terkoneksi, gunakan aplikasi *Browser* dan mengetikkan alamat IP mesin fotokopi pada *url Browser* Guna memanfaatkan layanan *remote UI*.
   - Langkah-langkah diabadikan pemotretan, pencatatan, *screen shoot.*

- Pencarian dan pengambilan artifak dilakukan oleh ahli forensik yang memiliki syarat ahli.

2. Analisis Bukti Digital

   Setelah mendapatkan file atau data digital yang diinginkan dari proses pemeriksaan di atas, selanjutnya data tersebut dianalisis secara detail dan komprehensif untuk menetapkan data-data yang berhubungan dengan kasus yang terjadi. Tugas analisis ini mencakup berbagai kegiatan, seperti identifikasi pengguna atau orang di luar pengguna yang terlibat secara tidak langsung, lokasi, perangkat, kejadian dan mempertimbangkan bagaimana semua komponen tersebut saling terhubung hingga mendapat kesimpulan akhir.

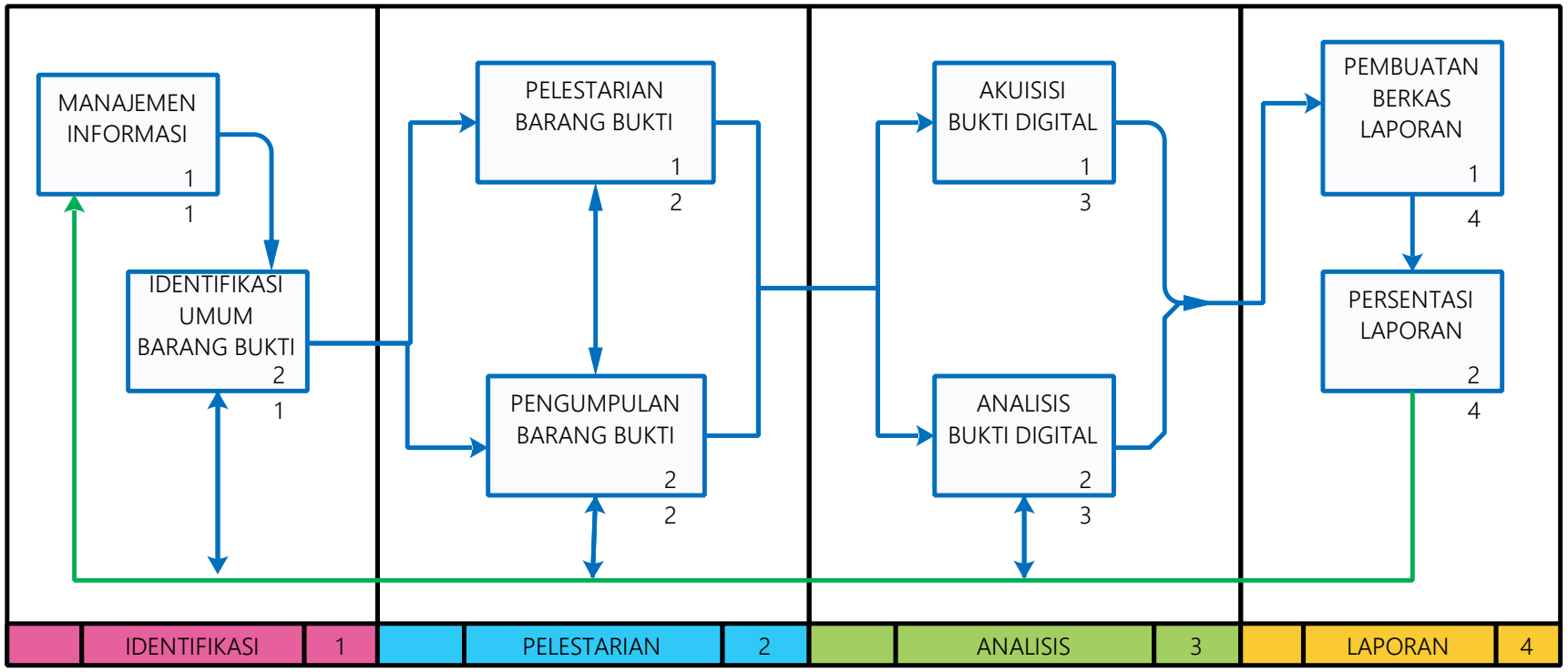
D. Laporan

1. Pembuatan berkas laporan berita acara pemeriksaan barang bukti yang dilakukan oleh ahli forensik, yang berisi:
   a. hasil yang ditemukan di tempat kejadian perkara baik saksi-saksi, tersangka maupun barang bukti.
   b. Tindakan yang dilakukan oleh petugas (tindakan pertama TKP dan pengolahan TKP) terhadap hasil yang ditemukan di tempat kejadian perkara.
   c. Sebagai bahan untuk pelaksanaan dan pengembangan investigasi selanjutnya
   d. Bahan bagi investigator lapangan selanjutnya.
   e. Pembuatan berita acara penemuan dan pengambilan jejak/bukti digital

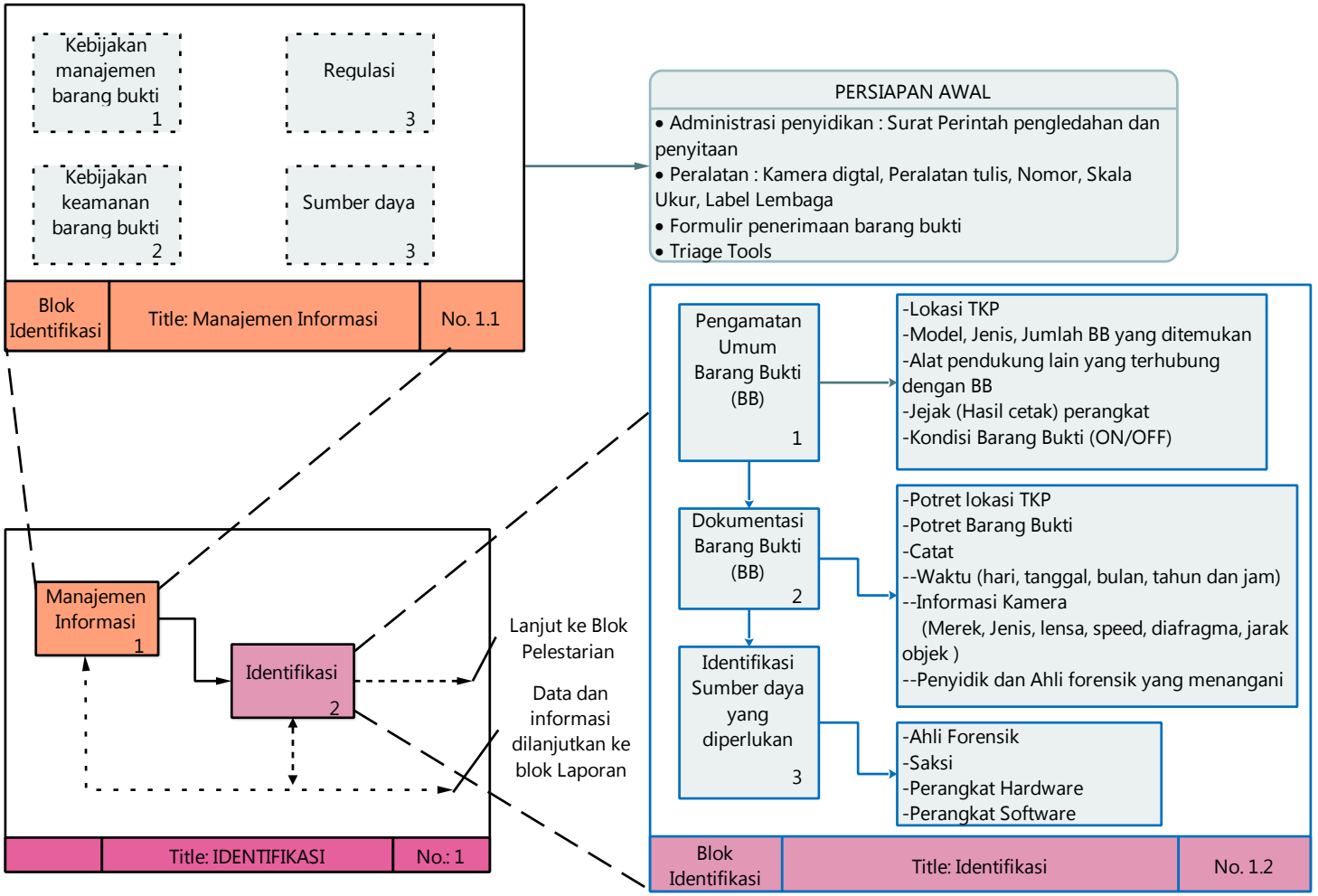
2. Presentasi Laporan : Menjadi ahli bila dibutuhkan

KERANGKA KERJA INVESTIGASI

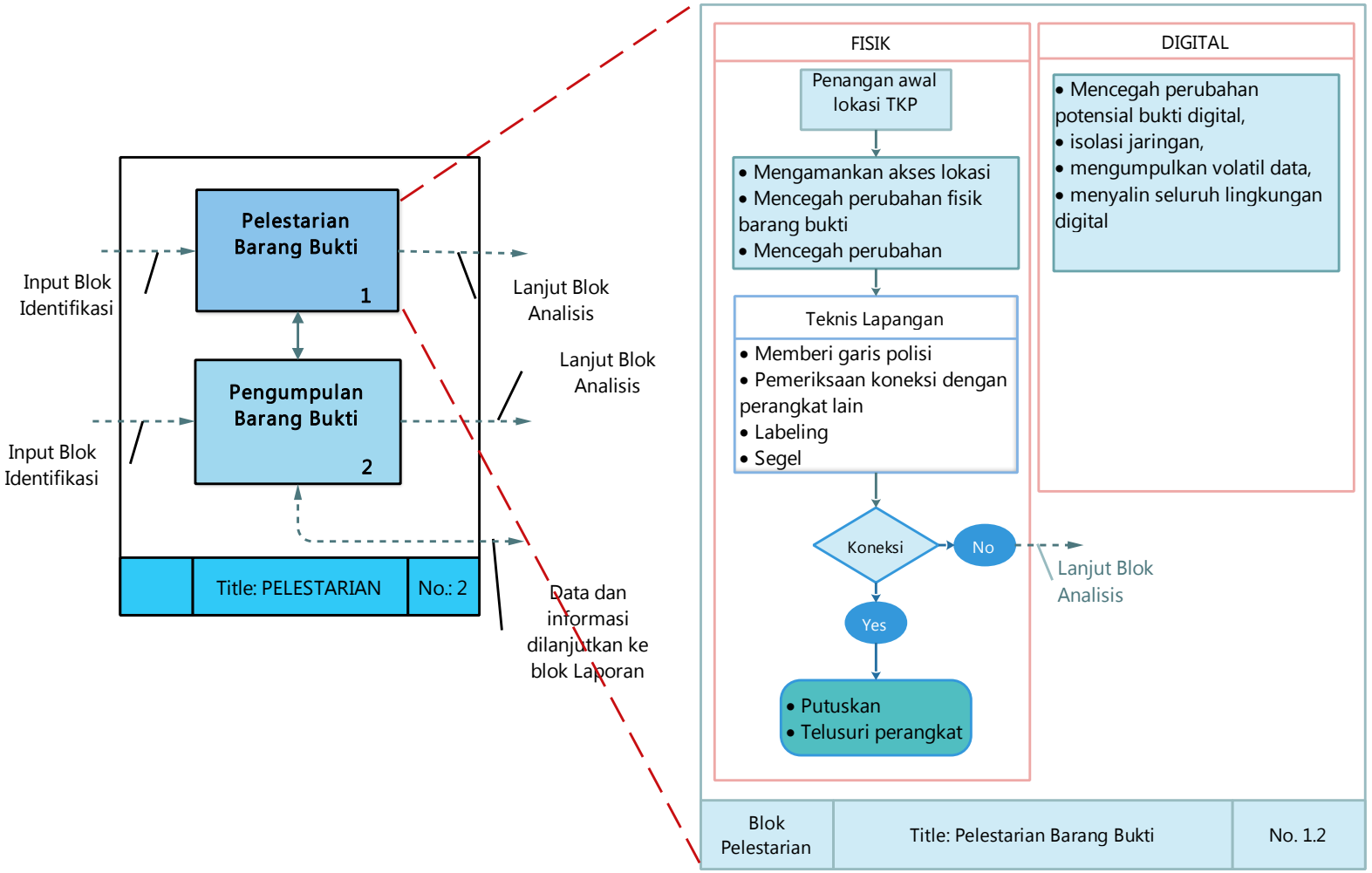
FORENSIKA DIGITAL MESIN FOTOKOPI MFP



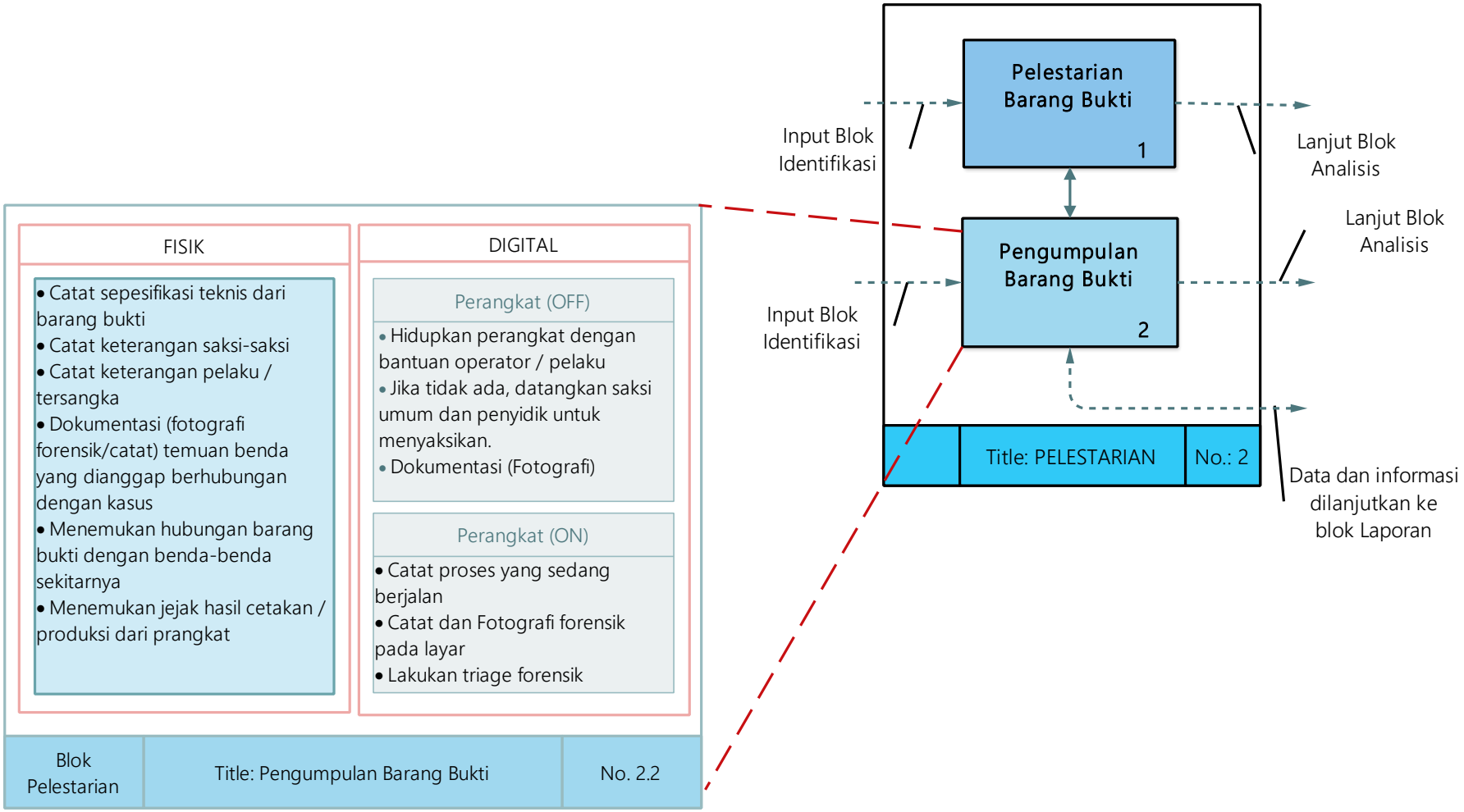
Gambar 4. 33 Kerangka kerja investigasi forensika digital mesin fotokopi MFP



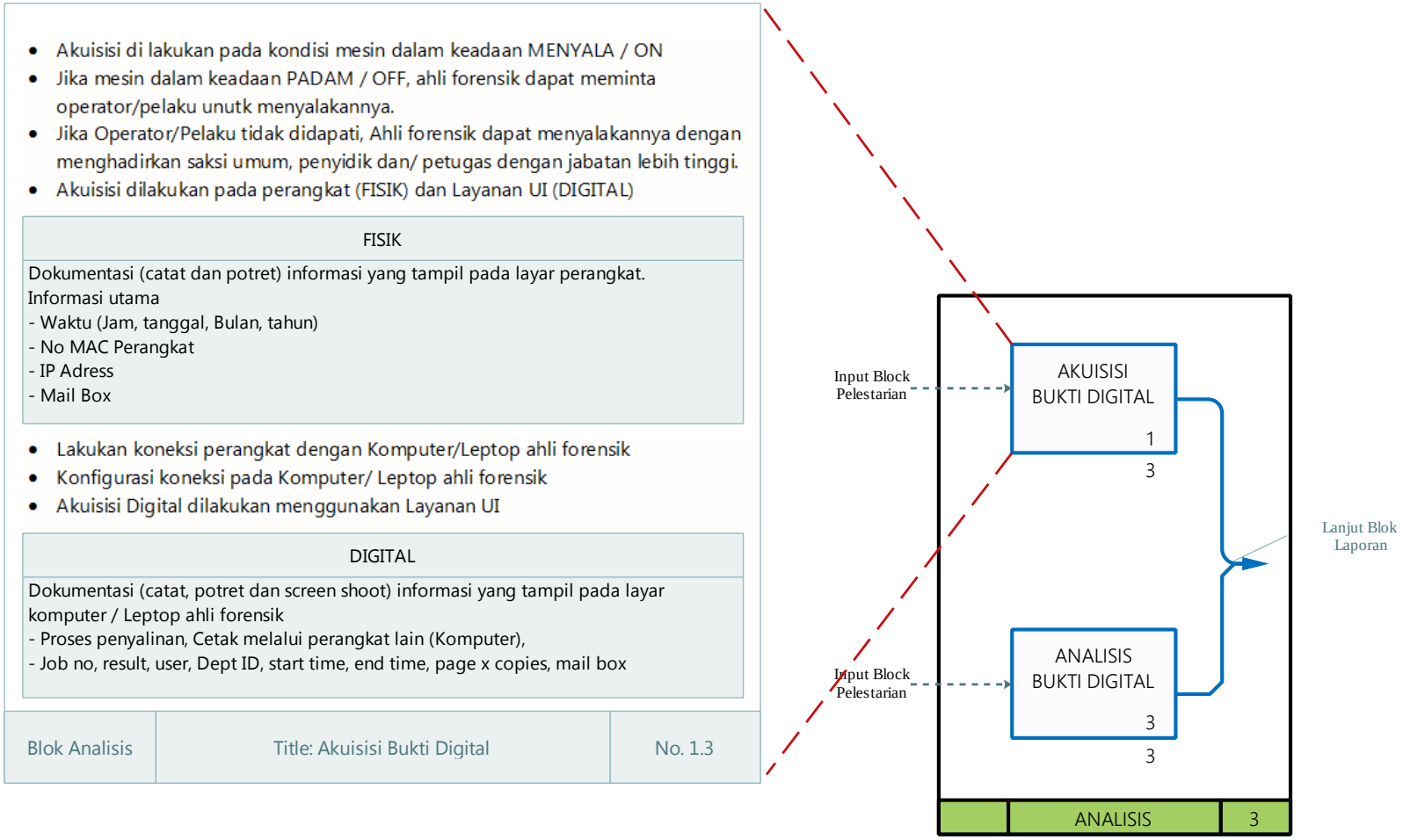
Gambar 4. 34 Kerangka Kerja Blok Identifikasi



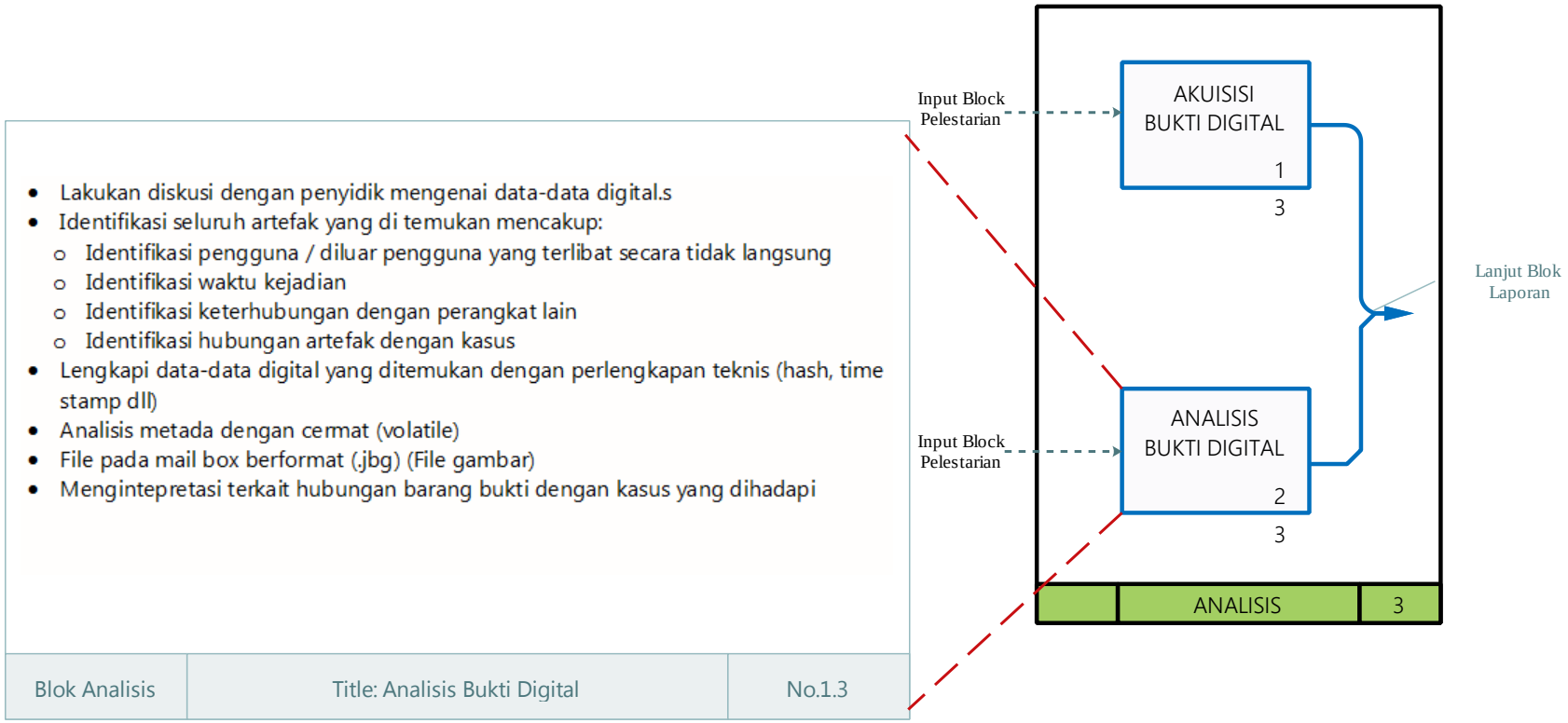
Gambar 4. 35 Kerangka Kerja Blok Plestarian sub-Plestarian Barang Bukti



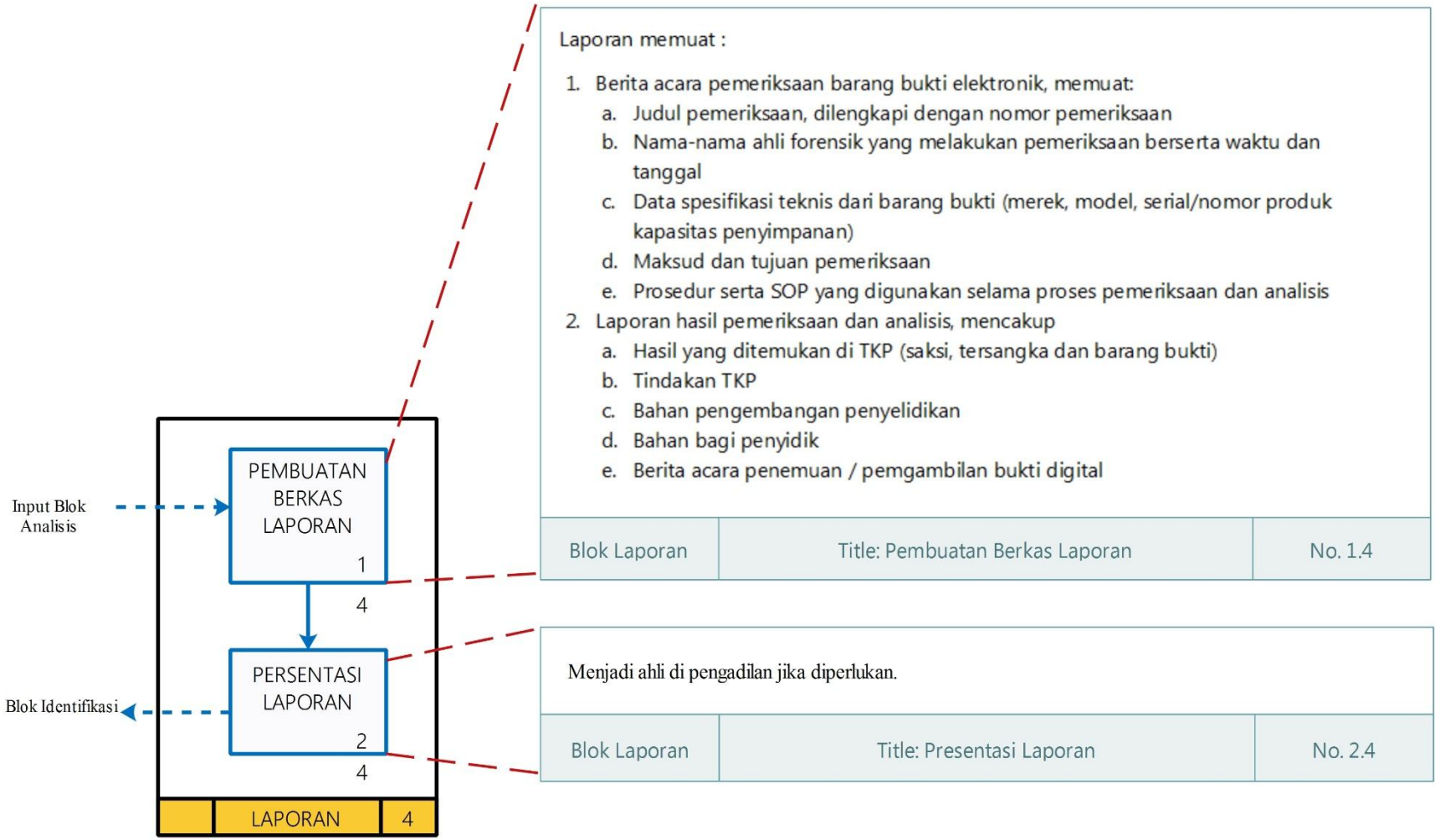
Gambar 4. 36 Kerangka Kerja Blok Plestarian, Sub-Pengumpulan Barang Bukti



Gambar 4. 37 Kerangka Kerja Blok Analisis sub-Akuisisi Bukti Digital



Gambar 4. 38 Kerangka Kerja Blok Analisis sub-Analisis Bukti Digital



Gambar 4. 39 Kerangka Kerja Blok Laporan

4.5 Penyelesaian Skenario Kasus Dengan Penerapan Kerangka Kerja Investigasi Forensika Digital Pada mesin Fotokopi MFP

Mesin fotokopi yang ditemukan diduga digunakan oleh pelaku sebagai alat untuk melakukan praktek ilegal tersebut. Bersumber dari skenario kasus sebelumnya (subbab 3.4) maka investigator dianggap belum mendapatkan bukti awal guna melanjutkan dugaan praktek percetakan buku ilegal, sementara di tingkat pengadilan Hakim tidak boleh menjatuhkan pidana kepada seorang kecuali apabila dengan sekurang kurangnya dua alat bukti yang sah ia memperoleh keyakinan bahwa suatu tindak pidana benar-benar terjadi dan bahwa terdakwalah yang bersalah melakukannya, yaitu (KUHAP pasal 183, 184 ayat (1)) :

Alat bukti yang sah ialah:

1. Keterangan saksi,
2. Keterangan ahli
3. Surat
4. Petunjuk
5. Keterangan terdakwa

Oleh sebab itu satu-satunya cara yang mungkin dilakukan oleh investigator adalah dengan mengakuisisi mesin fotokopi yang ditemukan pada saat pengledahan tersebut oleh seorang ahli forensika digital.

4.5.1 Mengapa Menggunakan Kerangka Kerja

Serangkaian kerangka kerja diterapkan dalam investigasi forensika digital mesin fotokopi tersebut, baik dari prosedur identifikasi umum barang bukti hingga proses pembuatan berkas laporan. Prosedur menjadi sangat penting untuk memastikan hasil akhir dari penyelidikan dapat diterima oleh hukum dan pengadilan oleh sebab itu maka penyelesaian skenario kasus ini mengikuti kerangka kerja Investigasi Forensika Digital Mesin Fotokopi MFP yang telah dirancang pada subbab sebelumnya.

1. **Manajemen Informasi Investigasi**

   Bersumber dari delik aduan CV. Cahaya Tulis, disinyalir sebagai tempat memproduksi buku ilegal. Oleh sebab itu pihak kepolisian mewacanakan untuk melakukan tindakan responsif (pengeledahan) sebagai bentuk pembuktian dari delik aduan tersebut, maka disiapkanlah persiapan-persiapan seperti administrasi, peralatan dokumentasi serta sumber daya yang diperlukan.

2. **Barang bukti yang diperiksa**

   Barang bukti elektronik yang diperiksa dari hasil pengledahan kantor percetakan CV. Cahaya Tulis pada hari SELASA tanggal 23 September 2014, berupa:

   a. 1 (satu) unit mesin fotokopi *Merk* Canon, Model iR 6000, *SN: NSN0796, MAC: 00008539e52c*

3. **Maksud Pemeriksaan**

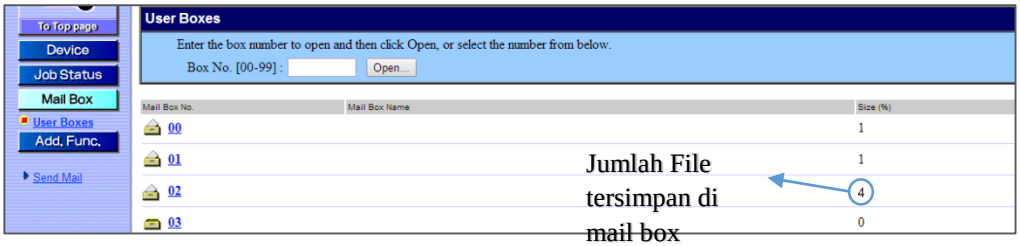
   Sesuai dengan permintaan Kepala Kepolisian pimpinan operasi pengledahan kantor percetakan CV. Cahaya Tulis pada hari Selasa tanggal 23 September 2014, untuk bantuan pemeriksaan secara digital barang bukti elektronik sehubung dengan tindak dugaan cetak ganda buku-buku secara ilegal. Buku yang dimaksud berjudul "Konsep Kecerdasan Buatan, oleh: Anita Desiani & Muhammad Arhami"

Hasilnya identifikasi pada salah satu mesin fotokopi didapatkan beberapa artifak yang diduga memiliki keterlibatan dalam praktek percetakan ilegal tersebut. Pemeriksaan barang bukti elektronik dilakukan dengan menerapkan konsep 5W1H sebagai dasar pemecahan masalah pada kasus ini.

4.5.2 Bagaimana Praktek Pembajakan Buku Tersebut Dilakukan

Analisis dilakukan guna mengetahui teknik yang dilakukan pelaku dalam menjalankan aksinya. Analisis dilakukan menggunakan layanan *remote UI* untuk memeriksa *log* pada *local copy* dan *mail box.* Barang bukti mesin fotokopi *Merk* Canon, model iR 6000, *SN: NSN0796, MAC: 00008539e52c,* investigator menemukan salah satu *folder mail box* berisi informasi yang berkaitan dengan

maksud pemeriksaan yaitu terdapat empat file berekstensi (*.jbg*) di sebuah folder pada *User Boxes (Mail box No. 02) size (%)* "4". Masing-masing file bernama 1.*001.jbg*, 2.*002.jbg* 3.*003.jbg* 4.*004.jbg*.



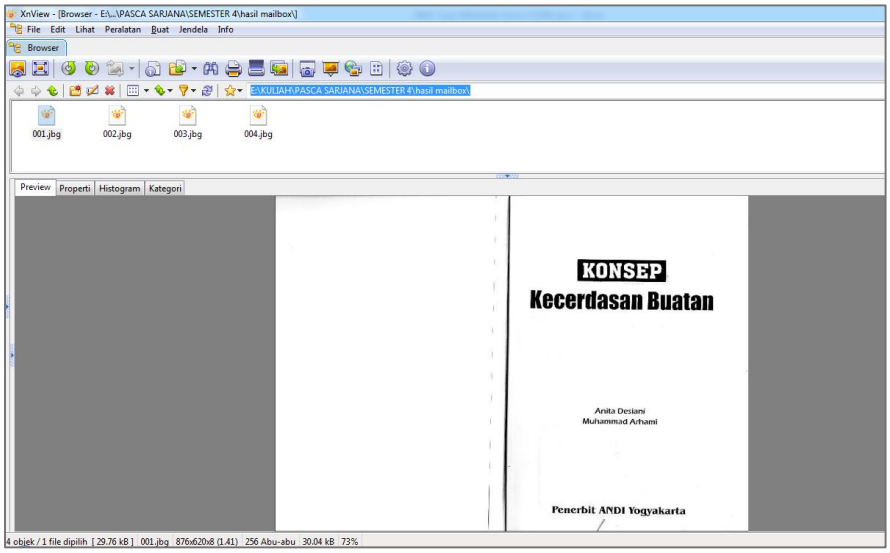
Gambar 4. 40 Tampilan *mail box* pada barang bukti

Selanjutnya folder tersebut diperiksa, sehingga peneliti menemukan beberapa file yang tersimpan.

Gambar 4. 41 File yang tersimpan pada *mail box*

Peneliti mencoba melakukan ekstraksi file tersebut, hasilnya ditemukan beberapa informasi penting yang berkaitan dengan kasus berupa gambar hasil *scan* dengan meta data sebagai berikut :

1. File pertama 001.jbg, memiliki informasi:
   - **FILE**_____
   - Nama File : *001.jbg*
   - Deskripsi : *JBG File*
   - Ukuran File : *30.471*
   - Dibuat : *12/07/2014 13:30*
   - Dimodifikasi : *12/07/2014 13:30*
   - **GAMBAR**_____
   - Format : *JBIG*
   - Lebar : *2544*
   - Tinggi : *2944*
   - #Bit : *2*
   - Model warna : *RGB*
   - Ukuran cetak : *21.87 x 30.90 cm, 8.61 x 12.17 inci*
   - Kompresi : *Nihil*
   - #Gambar : *1*
   - Asal : *Kiri-Atas*

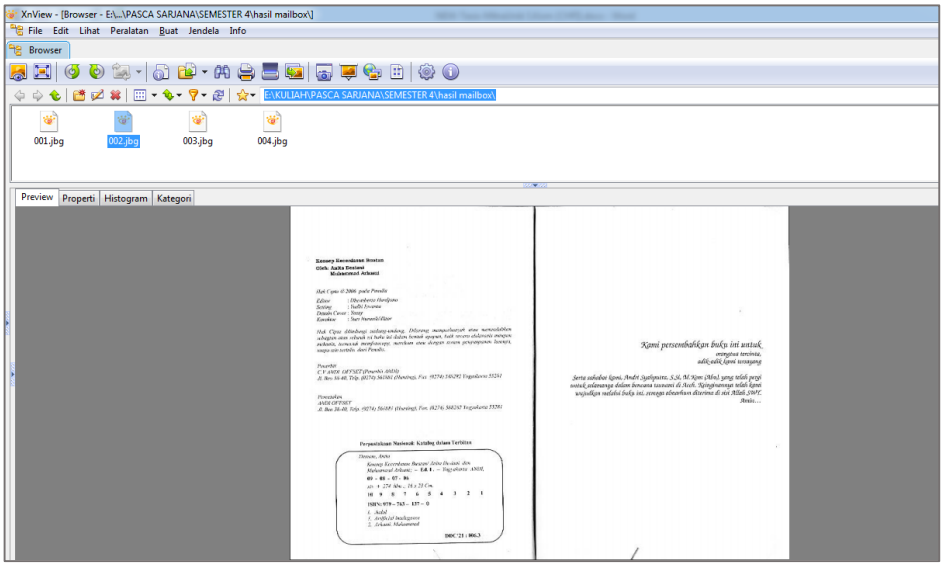


Gambar 4. 42 Tampilan file 001.jbg

Dari tampilan di atas ditemukan informasi yang berkaitan dengan kasus yang diusut. Tampilan seperti sebuah halaman awal buku dengan berikut tulisan: *KONSEP Kecerdasan Buatan* (Judul), *Anita Desiani & Muhammad Arhami* (Nama Orang) dan *Penerbit ANDI Yogyakarta* (Nama perusahaan Penerbitan)

2. File kedua 002.jbg, memiliki informasi

- **FILE_____**
- Nama File : *002.jbg*
- Deskripsi : *JBG File*
- Ukuran File : *69.047*
- Dibuat :
- Dimodifikasi : *12/07/2014 13:30*
- **Gambar_____**
- Format : *JBIG*
- Lebar : *2544*
- Tinggi : *2944*
- #Bit : *2*
- Model warna : *RGB*
- Ukuran cetak : *21.87 x 30.90 cm, 8.61 x 12.17 inci*
- Kompresi : *Nihil*
- #Gambar : *1*
- Asal : *Kiri-Atas*



Gambar 4. 43 Tampilan file 002.jbg

Dari tampilan di atas ditemukan informasi yang berkaitan dengan maksud penyelidikan. Tampilan seperti sebuah halaman buku yang berisi keterangan Hak Cipta dari buku tersebut di sebelah kiri dan tulisan persembahan. Selanjutnya pemeriksaan dilakukan dengan melihat *Copy Job Log*, guna mengetahui apakah telah terjadi pencetakan pada file yang diduga hasil *scan* buku yang diperkarakan.

Copy Job Log

Last Updated:12/07 2014 22:20:13

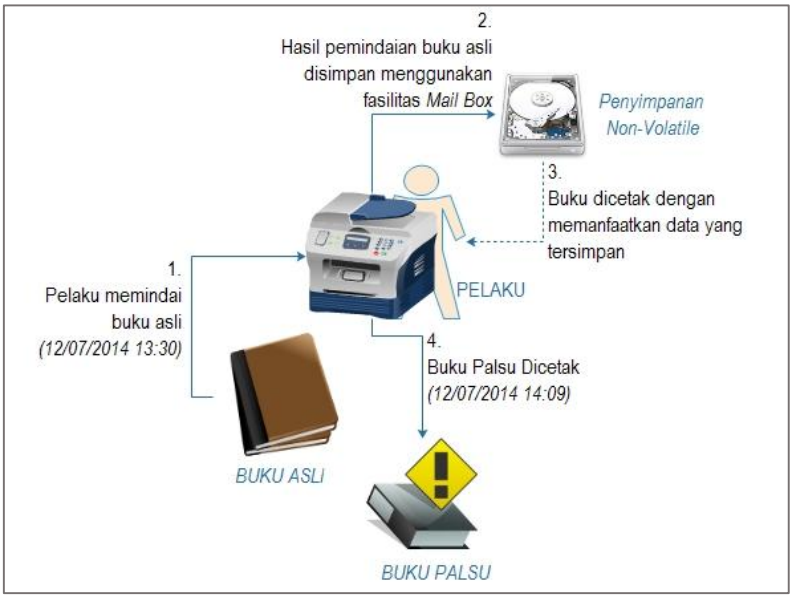
Job No.	Result	Dept. ID	Start Time	End Time	Pages x Copies
730	OK		12/07 2014 14:09:02	12/07 2014 14:10:01	4 x 1
729	NG		12/07 2014 14:07:05	12/07 2014 14:08:02	1 x 1
728	NG		12/07 2014 14:06:03	12/07 2014 14:07:03	1 x 1
727	OK		10/02 2014 13:07:05	10/02 2014 13:08:00	1 x 4
726	OK		10/02 2014 13:07:04	10/02 2014 13:07:05	1 x 1

Waktu cetak sesuai dengan metadata artefak pada *mail box*

Jumlah halaman sesusai dengan jumlah file pada *mail box*

Gambar 4. 44 Tampilan hubungan *copy log job* dan *mailbox*

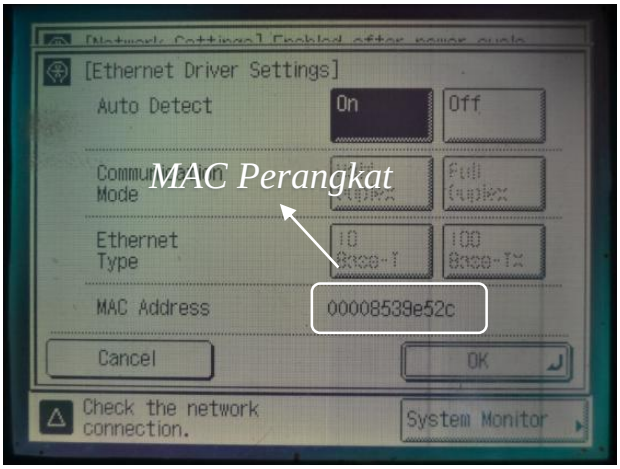
Berdasarkan hal tersebut dapat diambil kesimpulan bahwa pelaku merekam (*scan*) buku yang hendak digandakan ke dalam sistem *mail box* yang terdapat pada barang bukti elektronik, selanjutnya dilakukan pencetakan. Berikut gambaran umum skema aktivitas pembajakan pelaku.



Gambar 4. 45 Skema proses pembajakan buku

4.5.3 Identifikasi Alat yang Digunakan

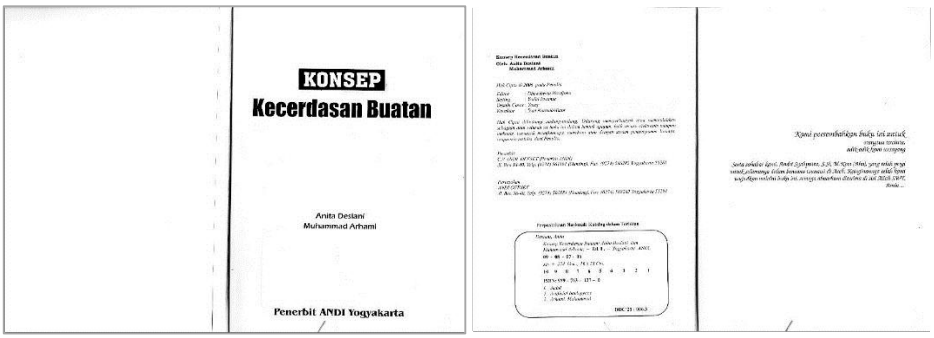
Pada kasus ini pelaku di identifikasi menggunakan perangkat mesin fotokopi *Multi Function Peripheral Merk* Canon, model iR 6000, *SN: NSN0796, MAC: 00008539e52c,*.



Gambar 4. 46 Mac Perangkat bukti elektronik

4.5.4 Identifikasi Data Objek

Pada kasus ini pelaku melakukan pelanggaran hak cipta dengan melakukan pembajakan buku yang berjudul "**Konsep Kecerdasan Buatan"**, penulis: "**Anita Desiani & Muhammad Arhami"** dan penerbit: **"Penerbit ANDI Yogyakarta".**



Gambar 4. 47 Bukti digital mengarah pada buku yang dimaksud dalam penyelidikan

4.5.5 Analisis Kesatuan Hubungan Barang Bukti dengan Pelaku

Dugaan sementara pelaku dalam kasus pembajakan buku ini adalah pemilik, pemimpin dan atau oknum operator yang masih berhubungan dengan CV. Cahaya Tulis. Karena lokasi tersebut merupakan lokasi operasi penggeledahan dilakukan.

4.5.6 Merekonstruksi Waktu Kejadian

Untuk mengetahui kapan tindak tersebut dilakukan dapat diketahui dari *log* saat dokumen / buku tersebut di pindai dan di cetak. *Log* tersebut di temukan saat pemeriksaan *remote UI.* Menurut hasil pemeriksaan tindak pelanggaran tersebut dilakukan pada tanggal 12 Juli 2014 waktu 14:09:02.

Gambar 4. 48 Artifak menunjukkan waktu yang dimaksud pada penyelidikan

4.6 Kesimpulan Skenario Kasus

Berdasarkan hasil pemeriksaan forensika digital pada skenario kasus maka dapat disimpulkan :

1. Pemeriksaan menemukan beberapa informasi dan artifak berupa rekaman waktu, jumlah cetakan serta file yang tersimpan pada penyimpanan *non-volatile.*
2. File berekstensi *(.jbg)* diketahui sebagai salah satu file berformat gambar.
3. File tersebut ditemukan merupakan hasil *scan* yang disimpan (*mailbox*) sebelum pekerjaan cetak dilakukan.
4. Bukti digital pada mesin fotokopi hanya berbentuk *log (user, time, job no* dan *result)* dan file yang tersimpan pada *mail box.*
5. Analisis pencocokan/hubungan berbagai artifak dengan kasus merupakan hal penting bagi penyelidikan kasus dengan barang bukti elektronik mesin fotokopi MFP.
6. Berdasarkan analisis yang didapat atas hasil pemeriksaan barang bukti elektronik (mesin fotokopi) yang ditemukan di TKP, bahwa percetakan dan penerbitan pada skenario kasus, diduga kuat terlibat dalam praktek penggandaan buku tanpa izin.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil penelitian ini maka dapat disimpulkan:

1. Teknik *static acquisition* dan *live acquisition* dapat lakukan pada mesin fotokopi MFP namun hanya teknik *live acquisition* yang mampu memberikan hasil guna membantu penyelidikan investigasi mesin fotokopi *Multi Function Peripheral* (MFP).
2. Beberapa kelompok artifak yang dapat di temui pada mesin fotokopi *Multi Function Peripheral* (MFP) adalah:
   a. Artifak proses penyalinan (*copy*)
   b. Artifak proses pencetakan dari komputer (*print*)
   c. Artifak proses pencetakan yang menggunakan jaringan LAN (*local Print*)
   d. Artifak pencetakan informasi dari mesin (*print report*)

   Dari keseluruhan kelompok artifak , dapat diketahui informasi-informasi seperti:

   - Nomor bilangan pekerjaan (*Job No*),
   - Keterangan Hasil (*result*),
   - Keterangan Pengguna (*User*),
   - Identitas Kelompok (*Dept Id*),
   - Waktu Mulai (*Start Time*) dan
   - waktu selesai (*End Time*).
   - Jumlah kertas yang disalin dalam sekali penyalinan (*page x copies*
   - *File* dokumen yang disimpan pada media *non-volatile. (mail box)*
3. Teknik akuisisi paling ideal yang dapat dilakukan pada investigasi mesin fotokopi MFP adalah dengan teknik *live acquisition.*

4. Kerangka kerja investigasi dapat dirancang setelah memperhatikan hasil dari penelitian ini.

5.2 Saran

Beberapa saran yang mungkin berguna bagi penelitian selanjutnya, antara lain:

1. Penggunaan Jenis mesin fotokopi yang berbeda sebagai objek penelitian.
2. Membahas mengenai struktur *file system* yang digunakan sesuai objek penelitian yang digunakan.
3. Menemukan cara *static acquisition* hingga didapatkan artifak yang juga mampu disuguhkan sebagai bukti digital.
4. Menerapkan kerangka kerja pada penelitian ini guna menguji validitas dan kesesuaian pada jenis mesin fotokopi MFP lainnya.

DAFTAR PUSTAKA

ACPO. (2012). *ACPO Good Practice Guide for Digital Evidence* (pp. 1–41).

Ademu, I. O., Imafidon, C. O., & Preston, D. S. (2011). A New Approach of Digital Forensic Model for Digital Forensic Investigation. *International Journal Of Advanced Computer Science and Applications*, 175–178.

Agarwal, A., & Gupta, M. (2011). Systematic digital forensic investigation model. *… Journal of Computer …*, *5*(1), 118–131.

Al Azhar, M. N. (2013). SOP on Digital Forensic. Retrieved April 22, 2014, from http://www.linkedin.com/groups/SOP-on-Digital-Forensic-4439573.S.229388439

Al-azhar, M. N. (2012). *Digital Forensic - Panduan Praktis Investigasi Komputer*. (P. Wuriarti, Ed.) (1st ed., p. 236). Jakarta: Salemba Infotek.

Andriono, B. (2013). *Makalah POLDA DIY*. Yogyakarta.

Bintariadi, B. (2007). Penjual Buku Jadi Tersangka Pembajakan Buku. *Tempo.co*. Retrieved July 04, 2014, from http://www.tempo.co/read/news/2007/12/21/058113942/Penjual-Buku-Jadi-Tersangka-Pembajakan-Buku

Businessdictionary. (2014). non-volatile memory. Retrieved April 12, 2014, from http://www.businessdictionary.com/definition/non-volatile-memory.html

Carrier, B., & Spafford, E. H. (2003). Getting Physical with the Digital Investigation Process, *2*(2), 1–20.

Casey, E., & Schatz, B. (2011). Conducting Digital Investigations. In *Digital Evidence and Computer Crime Third Edition* (third., pp. 187–227). Elsevier Inc.

CBSNews. (2010, April 19). Digital Photocopiers Loaded With Secrets. Retrieved March 21, 2014, from http://www.cbsnews.com/news/digital-photocopiers-loaded-with-secrets/

Clark, D. (2014). Why Instructional System Design and ADDIE? Retrieved November 24, 2014, from http://www.nwlink.com/~donclark/hrd/sat1.html

DeGaine, Jacqueline J, & Major. (2014). Digital Evidence. In *The Army Lawyer* (pp. 1–17). United States: Superintendent of Documents. doi:1448189974

Edrm.net. (2005). EDRM. Retrieved December 01, 2014, from http://www.edrm.net/resources/edrm-stages-explained

Eka Surya, D. (2014). Cara Mengadakan Penelitian.

Eko Indrajit, R. (2014). Forensik Komputer.

Encyclopaedia Britania. (2014). photocopying machine. Retrieved April 23, 2014, from http://www.britannica.com/EBchecked/topic/457786/photocopying-machine

Erlangga, P. (2013). Perlindungan Hukum Hasil Karya Cipta Buku Terhadap Bentuk-Bentuk Pembajakan. Retrieved March 16, 2014, from http://www.erlangga.co.id/umum/7616-perlindungan-hukum-hasil-karya-cipta-buku-terhadap-bentuk-bentuk-pembajakan.html

Fotocopy Global. (2013). Mesin Fotokopi Canon. Retrieved November 22, 2014, from http://globalfotocopy.com/review/mesin-fotocopy-canon-cepat-rusak/

Ifaorumhe, B. (2009). A SURVEY OF PHOTOCOPYING PRACTICES IN SOME SELECTED UNIVERSITIES IN WESTERN NIGERIA. *Ozean Journal of Social Sciences 2*, *2*(2), 115–127. Retrieved from http://www.ozelacademy.com/OJSS_v2n2_timmy.pdf

Katano, S. (2004). MULTI-FUNCTION PERIPHERAL. United States.

Kitab Undang-Undang Hukum Acara Pidana (KUHAP) Undang-Undang Nomor 8 Tahun 1981. (1981).

Kuhn, M. (2002). JBIG1 patent information. Retrieved January 06, 2015, from http://www.cl.cam.ac.uk/~mgk25/jbigkit/patents/

L.Levin, B., Dalrymple, J. C., & Dolan, J. E.-. (2007). SYSTEM FOR IMPROVING DIGITAL COPLERS AND MULTIFUNCTION PERIPHERAL DEVICES. United States.

McKemmish, R. (1999). What is forensic computing? *Trends and Issues in Crime and Criminal Justice*, *118*, 1–6. Retrieved from http://www.aic.gov.au/publications/current series/tandi/101-120/tandi118.html

Merrill, R. a, Bartick, E. G., & Taylor, J. H. (2003). Forensic discrimination of photocopy and printer toners I. The development of an infrared spectral library. *Analytical and Bioanalytical Chemistry*, *376*(8), 1272–8. doi:10.1007/s00216-003-2073-0

Metode Komputer Forensik. (2012). Universitas Gunadarma. Fakultas Teknologi Industri, Jurusan Teknik Informatika. Retrieved from C:\Users\ASUS\Downloads\Documents\M05_ Metode Komputer Forensik.ppt

Mizuyama, Y. (2007). *Image* Data Stronge Device, Photocopier, *Image* Forming System, and *Image* Data Stornge Method. United States.

Poentoadji, A. (1990). *Simulasi control fotocopy dengan menggunakan komputer IBM PC*. Universitas Kristen Petra, Surabaya.

Pollitt, M. M. (1995a). Computer forensics: An approach to evidence in cyberspace. In *Proceedings of the Eighteenth National Information Systems Security Conference* (pp. 487–491).

Pollitt, M. M. (1995b). Pinciples, Practices, and Procedures: An Approach to Standards in Computer Forensics. *Second International Conference on Computer Evidence*, 10–15.

Pollitt, M. M. (2009). DIGITAL FORENSICS AS A SURREAL NARRATIVE. In G. Peterson (Ed.), *Advances in Digital Forensic V* (Vol. 306, pp. 3–15).

Prasetyo, Z. K. (2012). Research and Development, Pengembangan Berbasis Penelitian (pp. 4–5).

Reith, M., Carr, C., & Gunsch, G. (2002). An Examination of Digital Forensic Models. *International Journal of Digital Evidence*, *1*(3), 1–12.

Rouse, M. (2011). multifunction peripheral (MFP). *Whatls.com*. Retrieved August 13, 2014, from http://whatis.techtarget.com/definition/multifunction-peripheral-MFP

Ryan, V. . (2010). Printing Processes -THE Photocopier, 1–2.

Tanner, A., & Dampier, D. (2009). CONCEPT MAPPING FOR DIGITAL FORENSIC INVESTIGATIONS. In G. Peterson & S. Shenoi (Eds.), *Advances in Digital Forensics V* (pp. 291–300). Springer Berlin Heidelberg. doi:10.1007/978-3-642-04155-6_22

Technopedia. (2014). Techopedia explains Multifunction Peripheral (MFP). Retrieved April 25, 2014, from http://www.techopedia.com/definition/3611/multifunction-peripheral-mfp

UU RI Nomor 11 Tahun 2008, Tentang Informasi dan Transaksi Elektronik. (2008). *Vasa*. Kementrian Hukum dan HAM Republik Indonesia. Retrieved from http://medcontent.metapress.com/index/A65RM03P4874243N.pdf

UU RI Nomor 19 Th 2002, Tentang Hak Cipta. (2002). Indonesia. Retrieved from http://www.dgip.go.id/

Virtualizationadmin. (2014). Fixing Rollers. Retrieved April 25, 2014, from http://www.virtualizationadmin.com/files/whitepapers/ultimate_printer_manual/glossdfs.htm

Whatls.com. (2014). Definition Multifunction Peripheral (MFP). Retrieved April 25, 2014, from http://whatis.techtarget.com/definition/multifunction-peripheral-MFP

Wikipedia. (2014). Mesin Fotokopi. Retrieved April 23, 2014, from http://id.wikipedia.org/wiki/Mesin_fotokopi

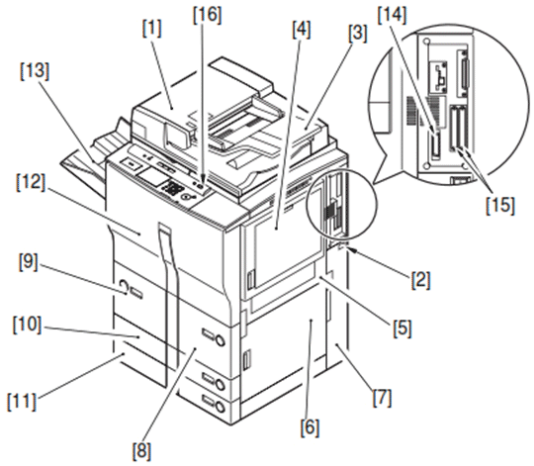
Willassen, S. Y. (2014). Forensic analysis of digital copiers. Retrieved March 16, 2014, from http://www.willassen.no/svein/pub/copier-en.pdf

Yasinsac, A., Erbacher, R., Marks, D., Pollitt, M., & Sommer, P. (2003). Computer forensics education. In *IEEE Scurity and Privacy* (Vol. 1, pp. 15–23).

LAMPIRAN

1. **Spesifikasi Canon iR6000 *Multi Function Peripherals***

   a. Skema Perangkat Canon iR6000



Gambar 1. Tampilan perangkat Canon iR 6000

Keterangan:

[1]	ADF	[8]	Right front paper deck
[2]	Main Power Switch	[9]	Left front paper deck
[3]	Original pickup tray	[10]	Cassette 3
[4]	Manual feed tray	[11]	Cassette 4
[5]	Right upper cover	[12]	Front cover
[6]	Right lower cover	[13]	Delivery tray
[7]	Waste toner box, grip drum protection sheet case	[14]	Parallel connector for downloading
		[15]	Slot for expansion board
		[16]	Control panel power switch

b. Panel Control Canon IR 6000

Gambar 2 Tampilan Panel Control Canon Ir 6000

Keterangan:

1. Counter Check Key
2. Display contras dial
3. Copy key
4. Mail box key
5. Scan key
6. Reset key
7. Number key
8. Energy saver key
9. Control panel power switch
10. Stop key
11. Start Key
12. Main power indicator
13. Clear key
14. Error lamp
15. Processing / data Lamp
16. ID key
17. Interrupt key
18. Additional Function Key
19. Guide Key
20. Touch panel
21. Clip holder

c. Spesifikasi Lengkap Canon Ir6000

TYPE:	DIGITAL MULTIFUNGSI IMAGING SYSTEM
Imaging System:	Laser transfer elektrostatik kering
Mengembangkan Sistem:	Dry Monocomponent Toner Proyeksi
Duty Cycle:	Hingga 200.000 [1] tayangan / bulan
Image Server Memory:	5.1GB (Standard) + 128MB RAM

TYPE:	**DIGITAL MULTIFUNGSI IMAGING SYSTEM**
Max. Kotak surat yang didukung:	100
Max. Salin Reservation:	5 Jobs
Scanning Resolusi:	600 dpi x 600 dpi
Mencetak Resolusi:	600 dpi x 600 dpi
Resolusi diinterpolasi:	1.200 dpi x 600 dpi (Copy) 2.400 dpi x 600 dpi (Print)
Halftone:	256 Gradasi Gray
Multicopy Kecepatan A4: A4-R: Hukum: Ledger:	 50 cpm / ppm 39 cpm / ppm 36 cpm / ppm 30 cpm / ppm
Beberapa Salinan (Rentang per pekerjaan):	1-999
Pembesaran:	25% - 400%, dengan penambahan 1%
Preset Penurunan: Preset Pembesaran:	25%, 50%, 64%, 73%, 78% 121%, 129%, 200%, 400%
Diterima Originals:	Lembar, Buku dan 3-Dimensi Objects ^{2} (max: 2 kg)
Maksimum Ukuran Asli:	A3
Standar Kertas Kapasitas:	2 x 550 Lembar + 2 x 1.500 Lembar

TYPE:	DIGITAL MULTIFUNGSI IMAGING SYSTEM
Manual Bypass:	50 Lembar
Maksimum Kertas Kapasitas:	7.650 Lembar
Ukuran masukan Kaset: Bypass:	B5 ke A3 A4 ke A3
Duplexing:	Standar Automatic Duplexing trayless
Pemanasan Waktu:	5 Menit atau Kurang
Exposure Control:	Otomatis atau Manual (Teks, Foto atau Teks & Foto)
Daya Persyaratan:	115V, 60Hz (Step-down Transformer Needed)
Dimensi (H x W x D):	1136mm x 643mm x 743mm
Berat:	Sekitar 210 kg
Tipe Perangkat	Printer / Copier / Scanner
Tipe Copier	Digital
Koneksi ke PC	-YES (LAN)
Menggunakan DIMM unit utama (192MB Standard)	Menggunakan DIMM unit utama (192MB Standard)
Koneksi antarmuka:	Ethernet (10/100BaseT) IEEE 1284 (Paralel)
Protokol yang didukung:	TCP / IP Appletalk
Processor:	Menggunakan unit utama Canon Kustom Processor (250MHz)