Sistem Monitoring Bukti Digital Untuk Meningkatkan Kontrol Terhadap Kasus *Cybercrime* Di Indonesia

Krisna Widatama*
Teknologi Informasi, Universitas Muhammadiyah Purworejo, Purworejo 54111, Indonesia

ABSTRAK

Kemajuan teknologi komputer saat ini telah berkembang sangat pesat. Kemajuan tersebut memberikan dampak positif yaitu setiap orang dapat semakin terbantu terhadap pekerjaan yang diakukan. Selain itu, jenis lapangan pekerjaan yang tersedia menjadi bertambah. Dibalik dampak positif tersebut terdapat juga dampak negatif, misalnya semakin berkembangnya kejahatan komputer yang terjadi. Penanganan kejahatan komputer tersebut akan ditangani dimana tempat kejahatan komputer tersebut terjadi yaitu pada Tingkat Kecamatan (POLSEK).

Permasalahan yang terjadi adalah tidak semua instansi kepolisian di Tingkat Kecamatan memiliki alat untuk melakukan investigasi bukti digital terhadap kejahatan komputer. Sehingga prosedur yang sering dilakukan adalah mengirim bukti fisik tersebut ke Tingkat Daerah (POLDA) untuk diakuisisi dan dianalisis. Hal ini berakibat kepada rentannya bukti digital tersebut diakuisisi dan dimanipulasi saat bukti fisik tersebut dikirim ke Instansi Kepolisian di Tingkat Daerah oleh pihak yang tidak memiliki wewenang. Berdasarkan permasalahan tersebut, diperlukan adanya pembaharuan terhadap prosedur penanganan bukti digital apabila terjadi kasus kejahatan komputer serta sistem yang terintegrasi antar kedua instansi tersebut.

Hasil dari penelitian ini adalah sebuah prosedur penanganan bukti digital melalui sebuah sistem monitoring terpadu antara instansi POLSEK dan POLDA. Diharapkan melalui sistem monitoring ini, bukti digital dapat terjaga keasliannya dan dapat dipertanggungjawabkan di pengadilan.

***Kata Kunci**: Bukti digital, Bukti fisik, Kejahatan komputer*

ABSTRACT

Nowadays, the computer technology is growing rapidly. This has a positive impact, many people can be helped by the computer. In addition, the types of jobs available are increasing. But, there are also negative impacts, for example the computer crimes are growing dramatically. The komputer crimes will be handled where the place of computer crime occurred at the District Level (POLSEK). The problem occurs is when police agencies at the District Level do not have tools to investigate digital evidence. So the procedure to handle this computer crime is send the physical evidence to the Regional Level (POLDA) to be acquired and analyzed.

It will make the digital evidence vulnerable to be acquired and manipulated when the physical evidence is sent to the Regional Police Agency by people who do not have authority. It is necessary to renew the procedure for handling digital evidence in the case of a computer crime and integrated system between them.

This study will produce a procedure for handling digital evidence through an integrated monitoring system between POLSEK and POLDA agencies. It is hoped that through this monitoring system, authenticity can be maintained and the digital evidence can be accepted by judge in the court.

***Keywords**: Computer crime, Digital evidence, Physical evidence*

1. PENDAHULUAN

Munculnya kejahatan komputer bermula dari berkembangnya jaringan internet yang digunakan secara masif di seluruh dunia baik di institusi pemerintahan maupun swasta. Berkembangnya penggunaan jaringan internet ini juga mendorong pesatnya jenis sistem informasi yang bermunculan (Jaishankar, 2018). Kejahatan *Cybercrime* dibagi ke dalam 3 kelompok (Agus & Riskawati, 2016), yaitu:

1. *Cyberpiracy* merupakan suatu pembajakan dengan cara menggandakan perangkat lunak atau mendistribusikan suatu informasi melalui jaringan komputer.
2. *Cybertrespass* merupakan suatu kejahatan komputer yang berfungsi untuk mendapatkan hak akses ke sebuah sistem komputer.
3. *Cybervandalism* merupakan kejahatan komputer dengan cara melakukan penyerangan terhadap sistem komputer dengan satu program tertentu.

Ketika terjadi sebuah kejahatan komputer, maka terdapat 2 bukti yang akan disita oleh pihak kepolisian, yaitu bukti digital (*digital evidence*) dan bukti fisik (*physical evidence*).

Bukti digital merupakan bukti yang didapat dari perangkat komputer maupun perangkat penyimpanan komputer, seperti Harddisk, Flashdisk maupun Telepon Seluler (Roscini, 2016). Sehingga ketika terjadi suatu tindak kejahatan komputer, maka kedua bukti tersebut harus diperoleh untuk mendukung penyelidikan atas tindak kejahatan tersebut. Penanganan pada kedua bukti digital tersebut memiliki perbedaan, bukti digital dapat disimpan pada komputer maupun pada media penyimpanan lainnya karena bukti digital berbentu *file*, sedangkan pada bukti fisik disimpan pada ruangan khusus yang dapat menjaga bukti fisik tersebut dari kerusakan.

Penanganan kasus pada kejahatan komputer memerlukan satu prosedur dan peralatan tertentu yang berfungsi untuk mendapatkan bukti digital yang dapat mendukung terselesaikannya sebuah kasus kejahatan komputer. Setiap negara memiliki prosedur penanganan kasus kejahatan komputer yang berbeda-beda, sehingga tidak terdapat standar baku yang secara internasional yang dapat digunakan oleh setiap negara (Reith, Carr, & Gunsch, 2002). Meskipun demikian, beberapa prosedur penanganan kejahatan komputer telah dirangkum menjadi satu prosedur yang baru (Yusoff, Ismail, & Hassan, 2011). Prosedur tersebut meliputi 5 aktivitas utama, yaitu:

1. *Pre-process*
   Kegiatan yang berisi aktivitas persiapan alat untuk pengambilan bukti digital.
2. *Acquisition* and *Preservation*
   Kegiatan yang berisi aktivitas untuk melakukan identifikasi, pengambilan serta pengiriman bukti digital.
3. *Analysis*
   Kegiatan investigasi yang dilakukan terhadap bukti digital yang diperoleh.
4. *Presentation*
   Kegiatan dokumentasi dengan format tertentu terhadap bukti digital yang diperoleh serta laporan hasil analisisnya.
5. *Post-process*
   Kegiatan yang dilakukan setelah suatu kasus kejahatan komputer dinyatakan ditutup. Kegiatan ini meliputi: penyimpanan bukti digital dan bukti fisik di tempat yang aman.

Bukti digital yang akan diakuisisi dari bukti fisik membutuhkan suatu *tools* tertentu. *Tools* tersebut tidak hanya digunakan untuk melakukan akuisisi, namun juga digunakan dalam proses analisis (Hibshi, Vidas, & Cranor, 2003). *Tools* tersebut dibuat untuk digunakan secara terbatas oleh investigator dalam pengungkapan kasus kejahatan komputer. *Tools* tersebut memiliki fitur untuk melakukan akuisisi dan analisis bukti digital. Beberapa *tools* tersebut dapat diunduh secara gratis, namun jika pengguna ingin mendapatkan fitur analisis, maka pengguna harus membeli lisensinya dengan harga yang relatif sangat mahal. Hal ini berdampak pada pembatasan pembelian

lisensi *tools* tersebut di setiap Polsek. Sehingga ketika terjadi *cybercrime*, maka bukti fisik tersebut akan dibawa ke Polda untuk dilakukan proses akuisisi hingga ke tahap analisis. Atau jika tidak, Polsek akan menyerahkan investigasi kasus *cybercrime* tersebut kepada pihak swasta. Hasil dari analisis tersebut selanjutnya akan diserahkan kepada Polsek, tempat dimana terjadinya kasus tersebut. Hal ini berdampak kepada integritas bukti digital tersebut yang dapat membuat bukti digital tersebut dapat ditolak saat persidangan. Bukti digital yang diperoleh dari proses akuisisi sangat rentan untuk dimanipulasi karena berbentuk file (Widatama & Yudi Prayudi, 2017). Kerentanan bukti digital ini menjadi sebuah kelemahan yang sangat fundamental apabila bukti digital ini diserahkan untuk dianalisis oleh pihak ketiga tanpa adanya suatu sistem yang terintegrasi.

Oleh sebab itu, diperlukan sebuah konsep mekanisme penanganan bukti digital dengan menggunakan sebuah sistem yang terintegrasi. Mekanisme baru yang diusulkan ini akan membuat penananganan kasus *cybercrime* akan lebih terkontrol. Selain itu, dengan adanya sistem yang terintegrasi, institusi kepolisian akan lebih mudah untuk mengetahui perkembangan kasus *cybercrime* yang terjadi di setiap daerah.

Sistem terintegrasi ini secara umum diterapkan pada kebutuhan bisnis dengan skala besar, contohnya adalah penerapan ERP (Enterprise Resource Planning) yang bertujuan untuk melihat pengeluaran, pemasukkan dan stok barang pada setiap divisi yang ada pada satu perusahaan. Sistem terintegrasi yang diterapkan pada penanganan kasus *cybercrime* bertujuan untuk menjaga integritas bukti digital, sehingga bukti digital tersebut dapat diterima di persidangan. Setidaknya terdapat 4 kriteria sebuah barang bukti dapat diterima di pengadilan (Prayudi, Ashari, & Priyambodo, 2014), yaitu: *admissible, authentic, complete, reliable* dan *believable*).

a. *Admissible*
   Barang bukti yang diajukan harus memiliki kesesuaian dengan fakta dan masalah yang terjadi. Selain itu, barang bukti tersebut dapat diterima di pengadilan.
b. *Authentic*
   Barang bukti yang diajukan di pengadilan harus sah dan legal tanpa sedikitpun rekayasa.
c. *Complete*
   Barang bukti yang diajukan harus lengkap. Hal ini bertujuan untuk membantu penyelesaian pengungkapan kasus.
d. *Reliable*
   Barang bukti yang diajukan harus dapat dipercayai. Aktivitas pengumpulan barang bukti harus sesuai prosedur yang berlaku.
e. *Believable*
   Barang bukti yang diajukan dan laporan hasil investigasi harus dimengerti oleh Hakim. Oleh karena itu, penggunaan istilah asing yang sulit dipahami harus dihindari.

Hal yang tidak kalah penting dalam penanganan bukti digital adalah proses dokumentasi atau biasa disebut sebagai *Chain of Custody* (Giova, 2011). Dokumentasi tersebut berisi setidaknya data bukti fisik dan bukti digital. Proses pembuatan *chain of custody* ini umumnya masih dibuat secara manual (belum terotomatisasi oleh *tools* tertentu). Selain itu, format chain of custody tidak baku, artinya setiap institusi bebas membuat dokumentasi dengan formatnya masing-masing. Meskipun demikian, beberapa *tools* yang digunakan saat penanganan kasus *cybercrime* telah memiliki fitur untuk membuat chain of custody yang didalamnya terdapat data rinci mengenai bukti fisik dan bukti digital.

2. METODE

Perancangan sistem ini menggunakan beberapa tahapan yang harus dilalui. Tahapan-tahapan ini dibuat untuk memastikan bahwa konsep sistem ini dapat diterapkan di kemudian hari. Gambar 1 menunjukkan metodologi yang digunakan dalam penelitian ini.

Gambar 1. Tahapan Penelitian

2.1. Literature Review

Proses ini bertujuan untuk mencari sumber tentang teori dasar forensika digital, hingga sistem terintegrasi. Sumber teori dasar yang diperoleh bersumber dari bahan bacaan, berupa: buku dan jurnal. Selain itu, sumber teori juga diperoleh melalui seminar-seminar yang terkait dengan bidang teknologi informasi dan forensika digital.

p-ISSN 2620 – 4843
e-ISSN 2620 – 4924

2.2. Perancangan Pengguna

Berdasarkan sistem yang akan dibuat, terdapat beberapa aktor yang akan berinteraksi terhadap sistem dan bukti fisik atau bukti digital. Aktor-aktor tersebut merupakan pengembangan dari aktor yang terlibat dalam *cybercrime* versi ACPO (Association of Chief Police Officers) yang berpusat di Inggris. Instansi ini sering dijadikan rujukan dalam hal penanganan *cybercrime* yang terjadi di beberapa negara termasuk di Indonesia. Tabel 1 berikut menjelaskan peran setiap aktor dalam penanganan *cybercrime* yang dibuat untuk memenuhi kebutuhan sistem.

Tabel 1. Rancangan pengguna

Aktor	Peran
Officer	Operator sistem yang berasal dari petugas POLSEK dan petugas POLDA.
First Responder	Petugas Kepolisian yang bertugas mengambil barang bukti di TKP dan melakukan proses akuisisi terhadap bukti fisik.
Penyidik	Petugas Kepolisian/swasta yang bertugas menganalisis dan menemukan bukti-bukti (bentuk *file*) dalam bukti digital untuk mendukung kasus. Ia juga berperan dalam membuat dokumentasi (Chain of Custody) untuk diserahkan ke Hakim sebelum persidangan berlangsung.

Selain ketiga aktor tersebut, terdapat aktor lainnya yang berperan sebagai pengawas terhadap kasus yang sedang ditangani, yaitu Pengacara. Aktor ini tidak memiliki akses terhadap sistem dan bukti fisik, namun ia dapat menggandeng pihak swasta untuk menganalisis bukti digital dengan meminta izin kepada pihak Kepolisian untuk menggandakan bukti digital serta ia juga dapat mengawasi kasus yang sedang ditangani melalui laporan dokumentasi yang dibuat oleh Penyidik. Dokumentasi yang dibuat berisi tentang prosedur, hasil analisis serta kesimpulan dari analisis bukti digital tersebut.

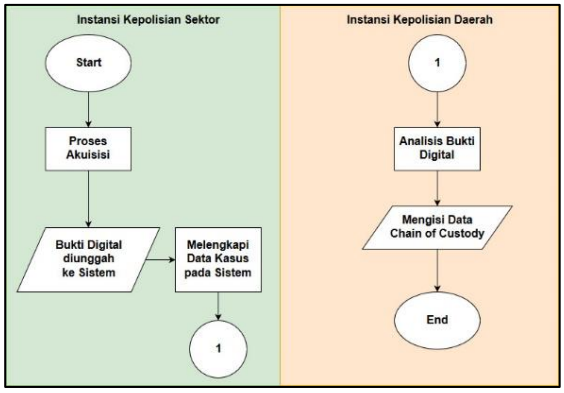
2.3. System Design

Tahap ini merupakan tahapan terakhir dari keseluruhan proses ini. Tahapan berisi aktivitas untuk merancang basis data berdasarkan simulasi kasus yang telah dibuat sebelumnya. Perancangan sistem yang dilakukan dapat mengakomodir segala macam jenis kasus yang berkaitan dengan *cybercrime*.

Perancangan sistem meliputi perancangan tabel pada basis data, perancangan alur penggunaan sistem. Penggunaan basis data pada sistem ini dikarenakan basis data dapat menyimpan data pada bukti digital menggunakan table yang saling berelasi, sehingga dapat dikembangkan apabila terdapat perubahan struktur tabel penyimpanan data bukti digital di masa yang akan datang. Basis data tidak bias berdiri sendiri, ia membutuhkan suatu DBMS (Database Management System). DBMS merupakan sebuah perangkat lunak tempat pengolahan data pada basis data di komputer.

2.4. Sistem Integrasi

Sistem integrasi yang diterapkan dalam penelitian ini adalah sistem integrasi antara sistem yang ada di instansi POLSEK dan instansi POLDA. Sistem integrasi ini bertujuan untuk memantau alur akuisisi yang dilakukan oleh instansi POLSEK telah sesuai dengan prosedur. Selain itu, sistem ini bertujuan untuk memastikan bahwa bukti digital yang dianalisis oleh pihak POLDA tidak dimanipulasi oleh pihak yang tidak berwenang. Berikut adalah alur penanganan *cybercrime* melalui sistem yang terintegrasi.



Gambar 2. Alur penanganan cybercrime

Gambar 2 menunjukkan alur penanganan *cybercrime*. Terlihat bahwa terdapat 2 instansi yang memiliki 2 peran yang berbeda. Instansi POLSEK memiliki peran untuk melakukan akuisisi. Hal ini karena diantara *tools* yang tersedia, *tools* tersebut memiliki kemampuan dasar akuisisi tanpa harus membeli lisensinya. Sehingga, semua instansi POLSEK dapat memiliki *tools* tersebut. Sedangkan kemampuan analisis bukti

digital dibebankan kepada instansi POLDA, hal ini karena *tools* untuk melakukan analisis bukti digital versi berbayar banyak tersedia di instansi POLDA yang ada di setiap daerah di Indonesia. Bukti digital yang telah selesai diakusisi, akan disimpan ke dalam server. Server tersebut menyimpan semua bukti digital yang terhadap satu kasus *cybercrime* yang terjadi di setiap daerah di Indonesia. Tiap Provinsi harus memiliki server khusus untuk penanganan bukti digital. Hal ini untuk membatasi hak akses terhadap bukti digital tersebut. Bukti digital hanya dapat diakses oleh daerah jangkauan instansi POLDA dimana terjadinya kasus tersebut. Selain itu, penyimpanan bukti digital melalui server terpadu, akan mencegah terjadinya duplikasi bukti digital yang dapat membuat bukti digital terebut rawan untuk dimanipulasi.

2.5. Perancangan Basis Data

Basis data pada sistem ini digunakan untuk melakukan penyimpanan data pada bukti fisik, bukti digital dan beberapa hal penting terkait kasus yang sedang dihadapi. Berikut adalah rancangan tabel yang digunakan untuk penyimpanan data.

Tabel 2. Tabel jenis_kasus

Kolom	Fungsi
idjenis_kasus	Primary Key pada tabel
jenis_kasus_rincian	Rincian jenis kasus

Tabel 2 menunjukkan rincian kasus yang ada di Indonesia. Tabel ini berfungsi untuk menyimpan pengelompokkan kasus yang sering terjadi di Indonesia.

Tabel 3. Tabel rincian_kasus

Kolom	Fungsi
idrincian_kasus	Primary Key pada tabel
rincian_kasus_detail	Rincian jenis kasus

Tabel 3 menunjukkan rincian jenis kasus pada tabel 2. Tabel 3 berfungsi untuk merincikan secara detail kasus yang ada pada tabel 2. Data pada tabel 2 dan tabel 3 telah ada sebelumnya.

Tabel 4. Tabel bukti_fisik

Kolom	Fungsi
idbukti_fisik	Primary Key pada tabel
jenis_bukti_fisik	Jenis bukti fisik (Flashdisk, Harddisk, dll.)
nama_bukti_fisik	Nama perusahaan pembuat bukti fisik
sn_bukti_fisik	Serial Number yang terdapat pada bukti fisik
kapasitas_bukti_fisik	Kapasitas penyimpanan pada bukti fisik
merk_bukti_fisik	Merek dagang dari bukti fisik.
warna_bukti_fisik	Warna bukti fisik
dimensi_bukti_fisik	Ukuran panjang atau layar bukti fisik
gambar_bukti_fisik	Link direktori penyimpanan gambar bukti fisik
imei_bukti_fisik	Nomor IMEI bukti fisik (umumnya ada pada Handphone)

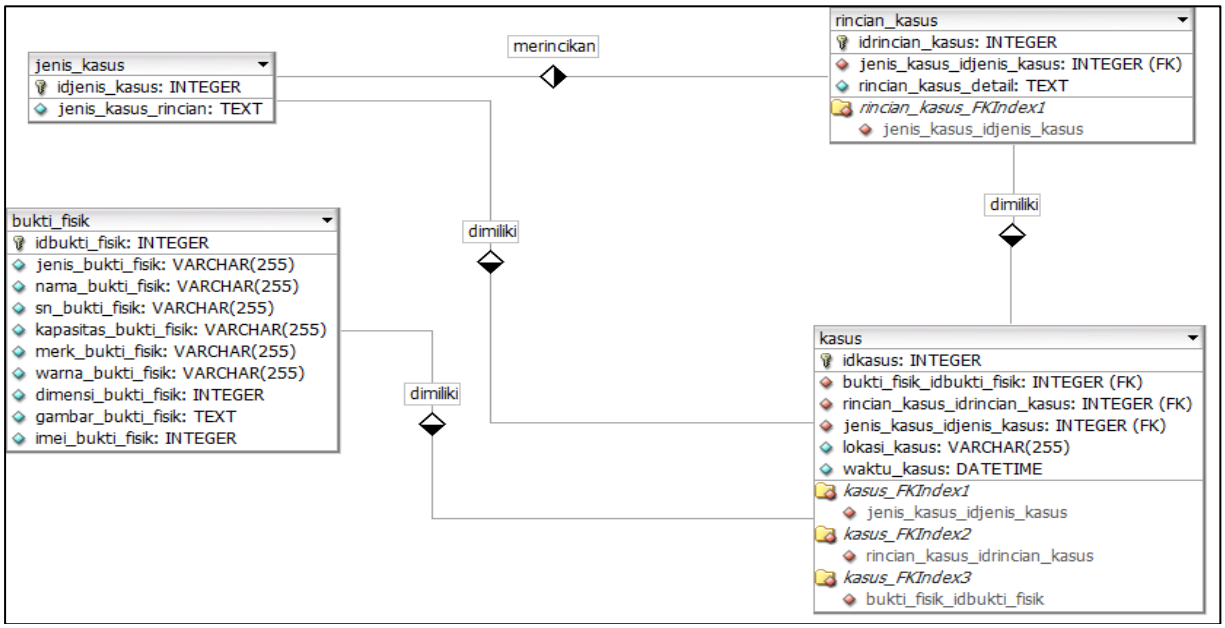
Tabel 4 berfungsi untuk menyimpan data bukti fisik. Tabel 5 berikut berfungsi untuk menyimpan beberapa data kasus yang akan disimpan.

Tabel 5. Tabel kasus

Kolom	Fungsi
idkasus	Primary Key pada tabel
nama_kasus	Nama kasus yang terjadi atau yang sedang ditangani
lokasi_kasus	Lokasi terjadi tempat kejahatan terjadi
waktu_kasus	Waktu terjadinya kasus tersebut

Keempat tabel tersebut saling berelasi satu sama lain. Relasi tabel terjadi karena data yang ada saling terkait satu sama lain. Gambar 3 menunjukkan relasi antar tabel.

p-ISSN 2620 – 4843
e-ISSN 2620 – 4924



Gambar 3. Relasi antar tabel pada sistem

Gambar 3 menunjukkan relasi antar tabel pada sistem. Relasi tersebut digunakan untuk melihat hubungan antar tabel. Tabel jenis_kasus berelasi dengan tabel kasus dan rincian kasus. Tabel bukti_fisik berelasi dengan tabel kasus. Semua tabel yang berelasi memiliki jenis relasi one to many yang artinya 1 data yang terdapat pada tabel asal dapat memiliki lebih dari satu kemunculan data pada tabel tujuan.

3. HASIL DAN PEMBAHASAN

Bab ini menjelaskan tentang pengujian sistem menggunakan satu simulasi kasus. Simulasi kasus yang digunakan merupakan kasus fiktif dimana nama dan tempat kejadiannya bukan kejadian sesungguhnya.

Cybercrime telah terjadi di Yogyakarta tepatnya pada tanggal 20 Februari 2019 pukul 20:00. Jenis *Cybercrime* yang terjadi adalah penipuan yang menyebabkan korban mengalami kerugian sebesar Rp. 2.000.000. First Responder mengamankan barang bukti fisik berupa sebuah Smartphone. Setelah mengamankan barang bukti, First Responder kemudian melakukan akuisisi bukti digital dan menghasilkan sebuah *file* akuisisi bernama *kasus_penipuan.dd* yang langsung disimpan ke dalam server. Hasil akuisisi tersebut kemudian disimpan ke dalam *database*. Berikut adalah isian data yang dimasukkan oleh First Responder.

idjenis_kasus	jenis_kasus_rincian
1	Kejahatan Terhadap Harta Benda
2	Kejahatan Terhadap Jiwa Seseorang
3	Kejahatan Terhadap Badan Seseorang
4	Kejahatan Mengenai Pemalsuan
5	Kejahatan Mengenai Kesusilaan
6	Kejahatan Terhadap Negara

Gambar 4. Data pada Tabel jenis_kasus

Data pada gambar 4 telah ada sebelumnya. First Responder dapat memilih jenis kasus yang terjadi berdasarkan jenis kasus yang terjadi. Berdasarkan simulasi kasus yang terjadi, maka jenis kasus yang dipilih adalah Kejahatan Terhadap Harta Benda dengan *idjenis_kasus* 1. Sedangkan pada tabel *rincian_kasus* merincikan kasus yang dikelompokkan dari tabel *jenis_kasus.* Berikut adalah data pada tabel *rincian_kasus.*

idrincian_kasus	idjenis_kasus	rincian_kasus_detail
1	1	Pencurian
2	1	Pencurian Khusus
3	1	Pemerasan
4	1	Pengancaman
5	1	Penipuan
6	1	Penadahan
7	1	Kejahatan Dengan Alat Percetakan

Gambar 5. Data tabel rincian_kasus

Gambar 5 merincikan jenis kasus Kejahatan Terhadap Harta Benda. First Responder dalam kasus ini memilih rincian Penipuan. Setelah memilih jenis dan rincian kasus, First Responder memasukkan data bukti fisik. Berikut adalah data bukti fisik yang didapat dari TKP.

Tabel 6. Data tabel bukti_fisik

Kolom	Data
idbukti_fisik	1
jenis_bukti_fisik	Smartphone
nama_bukti_fisik	Samsung
sn_bukti_fisik	097831093710
kapasitas_bukti_fisik	32 Gb
merk_bukti_fisik	Galaxy S5
warna_bukti_fisik	Putih
dimensi_bukti_fisik	5.5 Inch
gambar_bukti_fisik	C:\bd\image.png
imei_bukti_fisik	65463216106

Sedangkan data kasus disimpan pada tabel kasus. Berikut adalah data kasus pada tabel kasus.

Tabel 7. Data pada tabel kasus

Kolom	Data
idkasus	1
nama_kasus	Kasus Penipuan
lokasi_kasus	Yogyakarta
waktu_kasus	20-02-2019 20:00

Setelah data tersebut telah diisi oleh First Responder, pihak instansi POLSEK dapat mengajukan permohonan analisis bukti digital kepada instansi POLDA. Setelah bukti digital selesai dianalisis, hasil laporan analisis dapat diserahkan kepada instansi POLSEK.

4. SIMPULAN

Berdasarkan hasil perancangan dan pengujian dari simulasi kasus yang dibuat, maka dapat disimpulkan bahwa sistem yang terintegrasi antara pihak POLSEK dan POLDA dapat meningkatkan kontrol bukti digital pada sebuah kasus *cybercrime*. Integrasi sistem yang dibuat dapat mencegah terjadinya manipulasi bukti digital saat bukti digital tersebut dianalisis oleh pihak instansi POLDA. Hal ini karena bukti digital yang asli tersimpan di dalam server dan semua aktivitas terkait dengan unduh dan unggah bukti digital akan tercatat pada *log* server. Selain itu, dengan menggunakan konsep integrase monitoring ini juga akan memperjelas tugas dari instansi POLSEK dan instansi POLDA tentang penanganan bukti digital. Bahwa dalam penanganan bukti digital, instansi POLSEK bertugas untuk melakukan akuisisi dan pihak POLDA bertugas untuk melakukan analisis.

Penelitian ini belum memfokuskan terhadap prosedur unduh bukti digital yang dilakukan oleh pihak POLDA dalam analisis bukti digital. Sistem monitoring ini juga belum memiliki mekanisme terhadap pencatatan terhadap aktivitas unduh dan unggah bukti digital. Oleh sebab itu, mekanisme prosedur terhadap unduh bukti digital dari instansi POLDA dan skema pencatatan aktivitas unduh dan unggah bukti digital yang dilakukan oleh sistem menjadi 2 hal yang sangat penting untuk dilakukan dimasa yang akan datang.

DAFTAR PUSTAKA

Agus, A. A., & Riskawati. (2016). Penanganan Kasus Cyber Crime di Kota Makassar (Studi pada Kantor Kepolisian Resort Kota Besar Makassar). *Jurnal Supremasi*, *11*(1), 20–29.

Giova, G. (2011). Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems. *International Journal of Computer Science and Network Security*, *11*(1), 1–9. Retrieved from http://paper.ijcsns.org/07_book/201101/20110101.pdf

Hibshi, H., Vidas, T., & Cranor, L. (2003). Usability of Forensics Tools : A User Study.

Jaishankar, K. (2018). Cyber Criminology As An Academic Discipline: History, Contribution and Impact. *International Journal of Cyber Criminology*, *12*(1), 1–8.

Prayudi, Y., Ashari, A., & Priyambodo, T. K. (2014). Digital Evidence Cabinets : A Proposed Frameworks for Handling Digital Chain of Custody. *International Journal Of Computer Applications (IJCA)*, *109*(9), 30–36. https://doi.org/10.5120/18781-0106

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

Roscini, M. (2016). Digital Evidence as a Means of Proof before the International Court of Justice. *Journal of Conflict and Security Law*, *31*(3), 541–554.

Widatama, K., & Yudi Prayudi. (2017). Konsep Lemari Penyimpanan Bukti Digital Menggunakan Struktur Bahasa XML. *Seminar Nasional Informatika Dan Aplikasinya Ke-3*, (September), 23.

Yusoff, Y., Ismail, R., & Hassan, Z. (2011). Common Phases of Computer Forensics Investigation Models. *International Journal of Computer Science and Information Technology*, *3*(3), 17–31.