Jurnal INFORMA Politeknik Indonusa Surakarta p-ISSN : 2442-7942, e-ISSN 2716-5051
Vol. 6 Nomor 2 Desember 2020

Akuisisi Barang Bukti Digital Pada Smart CCTV Menggunakan Standarisasi ACPO DAN SNI ISO/IEC 27037:2014

Faulinda Ely Nastiti[1], Nindya Dwi Anggana[2], Heri Gunawan[3], Uning Kristiana[4]

[1]Universitas Duta Bangsa Surakarta, [2,3,4]Universitas Jenderal Achmad Yani Yogyakarta
[1]Jl. Bhayangkara no 55, Tipes, Serengan Surakarta
[2,3,4]Jl. Siliwangi, Ringroad Barat, Sleman, Yogyakarta
Email : faulinda.en@gmail.com

Abstrak

Pesatnya perkembangan yang semakin mempermudah akses internet perlu diwaspadai. Penyalahgunaan hak akses internet untuk keuntungan pribadi maupun merugikan orang lain termasuk kejahatan berbasis komputer. Kejahatan digital yang lebih biasa dikenal dengan Cybercrime sebagai bentuk dari aktivitas kejahatan yang menggunakan komputer atau jaringan komputer sebagai alat maupun tempat terjadinya kejahatan. Pada akhir 2016, terdata 400 juta Internet of things telah terkoneksi dengan ponsel dan jumlah tersebut diproyeksikan mencapai 1,5 miliar perangkat pada 2022 atau sekitar 70 persen dari kategori wide-area . Dalam bidang forensik, IoT sudah mulai banyak dimanfaatkan untuk membantu penyelidikan sebuah kasus kejahatan. Terdapat tiga ancaman keamanan pada IoT, yaitu keamanan fisik bagian sensor dan RFID dari intereferensi, operasi pada berbagai elemen yang harus dapat menjamin bahwa sensor dan sistem transmisi dan pengolah data tidak boleh di rusak, dicuri maupun dipalsukan. Smart CCTV yang merupakan bagian dari IoT sehingga dapat dikendalikan dari jarak jauh dimanapun dan kapanpun. Dalam penelitian ini kami membangun rumah cerdas sesuai dengan topologi yang kami buat. Peneliiti menggunakan sebuah smart CCTV merk Xiaomi tipe Xiaofang dan aplikasi yang terinstal pada ponsel cerdas yang bersistem operasi android adalah Mi Home. Dalam proses akusisi terdapat akuisisi secara fisik dari media penyimpan yang terpasang pada smart CCTV maupun ponsel cerdas, berupa image. Hasil image telah diverifikasi menggunakan hash untuk menjaga integritas barang bukti digital.

Kata kunci:*internet of things*, smart cctv, forensik digital, barang bukti digital, kejahatan digital.

1. PENDAHULUAN

Internet merupakan salah satu alat yang berguna dalam mempermudah mengakses dan mencari informasi. Dari fasilitas ini membawa dampak positif bagi pengguna internet dengan kegunaannya di berbagai hal (Nurzeni, 2009). Pesatnya perkembangan teknologi dan kemudahan akses intenet merupakan hal positif, namun juga perlu diwaspadai (Asosiasi Penyelenggara Jasa Internet Indonesia & Teknopreneur, 2018). Penyalahgunaan hak akses internet untuk keuntungan pribadi maupun merugikan orang lain termasuk kejahatan berbasis komputer. Kejahatan digital yang lebih biasa dikenal dengan *Cybercrime* sebagai bentuk dari aktivitas kejahatan yang menggunakan komputer atau jaringan komputer sebagai alat maupun tempat terjadinya kejahatan (Danuri & Suharnawi, 2017). Berdasarkan survey yang dilakukan oleh Numbeo, tingkat kejahatan yang terjadi di setiap negara berbeda-beda, termasuk di wilayah Asia Tenggara. Indonesia termasuk negara nomor lima yang memiliki sistem keamanan terkuat se-Asia tenggara, dengan peringkat pertama diduduki oleh negara Singapura. Indeks kejahatan yang ada di Indonesia mencapai nilai 46,26; sedangkan untuk indeks keamanannya menunjukkan indeks 53,74. Berdasarkan data tersebut membuktikan bahwa Indonesia belum banyak menerapkan sistem keamanan yang lebih kuat. Alasan Singapura menjadi negara paling aman nomor satu se-Asia Tenggara adalah karena Singapura telah menerapkan pengawasan dengan sistem CCTV di beberapa titik di setiap daerahnya, sehingga dimana kejahatan terjadi, maka akan lebih cepat terdeteksi dan tingkat kejahatan di sana semakin mengecil.

Perkembangan *Internet of Things (IoT)* memungkinkan hampir semua perangkat

dapat dihubungkan ke internet. Pada akhir 2016, terdata 400 juta IoT telah terkoneksi dengan ponsel dan jumlah tersebut diproyeksikan mencapai 1,5 miliar perangkat pada 2022 atau sekitar 70 persen dari kategori wide-area (Delgado, A.R., Picking, R. & Grout, 2006). Diperkirakan sampai dengan tahun 2022, pemanfaatan perangkat IoT meningkat sebesar 21% yang didorong oleh kebutuhan para pengguna, dan datangnya era Society 5.0. Dalam bidang forensik, IoT sudah mulai banyak dimanfaatkan untuk membantu penyelidikan sebuah kasus kejahatan. Terdapat ancaman keamanan pada IoT, yaitu keamanan fisik; kemanan ini befokus pada b sensor dan intereferensi RFID. Seluruh operasi harus menjamin bahwa system transmisi maupun sensor tidak boleh dirusak, dipalsukan, maupun dicuri. (Meutia, 2015). Smart CCTV yang merupakan bagian dari IoT sehingga dapat dikendalikan dari jarak jauh dengan waktu pada saat itu (Prabowo, Budiyanto, Nurcahyani, & Adinandra, 2018). Tujuan pemanfaatan Smart CCTV yaitu membantu dalam mengakses rekaman suatu lokasi dengan media pengakses smartphone bersistem operasi android. Oleh sebab itu jika terjadi suatu tindak kejahatan pada lokasi yang terekam menggunakan Smart CCTV perlu prosedur dan teknik akuisisi barang bukti yang sesuai dengan prosedur dan standar. Pada penelitian ini diusulkan teknik akuisisi barang bukti digital yang terdapat pada sistem Smart CCTV menggunakan standari ACPO dan SNI ISO/IEC 27037:2014.

2. TINJAUAN PUSTAKA

Proses CCTV merekam video atau audio dengan teknik mengirimkan sinyal secara broadcast melalui suatu media kabel maupun nirkabel. Kabel yang digunakan untuk CCTV biasanya menggunakan kabel coaxial atau kabel yang sering digunakan pada TV analog untuk menangkap sinyal broadcast dari antena TV. Sedangkan sinyal nirkabel yang digunakan yaitu frekuensi 2,4 GHz. Didalam CCTV terdapat Motion Detector yang berfungsi sebagai fitur untuk mengurangi beban penyimpanan data. Cara kerja Motion Detector adalah mendeteksi adanya perubahan pixel. Jika terjadi sebuah gerakan, maka kamera CCTV akan menganggap nilai pixelnya berubah dan akhirnya merekam perubahan tersebut. Hasil rekaman pada CCTV dengan dua metode yaitu Tape adalah media penyimpanan yang paling mudah dan hemat dan metode perekaman melalui Digital Video Recorders (DVR). DVR dibagi menjadi stand-alone DVR yaitu DVR yang mempunyai kamera dan tempat penyimpanan sendiri dan PC-based DVR yang media penyimpanannya disambungkan ke komputer. Dalam kasus persidangan adanya teknologi informasi CCTV dapat memudahkan hakim dalam menyelesaikan suatu perkara (Oliver, 2013).

CCTV adalah alat perekam situasional yang memungkinkan untuk hasilnya disimpan di bawah pengawasan jarak jauh. CCTV telah menjadi pencegahan dan kejahatan penting langkah keamanan. Kamera mengumpulkan gambar, yang ditransfer ke suatu perangkat seperti monitor yang berfungsi untuk diamati, ditinjau maupun disimpan. Sedangkan cara kerja kamera CCTV yaitu mengirimkan sinyal secara tertutup lewat melalui media nirkabel kabel. Ada banyak jenis sistem CCTV dan memiliki kapasitas berbeda untuk memenuhi berbagai tujuan (Gill & Spriggs, 2005).

IoT adalah segala bentuk fisik yang dapat terhubung ke internet dan perangkatnya dimanfaatkan untuk memantau dan mengendalikan sistem mekanis dan elektronik yang digunakan pada berbagai jenis bangunan, seperti industri atau perumahan. Selain itu juga dapat mengendalikan penggunaan energi secara real-time dalam mengurangi konsumsi energi (Davies, 2015).

3. METODE PENELITIAN

Metode akuisisi sistem Smart CCTV pada android berdasarkan standar SNI ISO/IEC 27037:2014. Tujuan utama dari standar ini adalah untuk memastikan keandalan dan kredibilitas bukti digital ketika barang bukti tersebut digunakan dalam kasus-kasus pengadilan dan perselisihan hukum (Buzarovska Lazetik & Koshevaliska, 2013).

Akuisisi sebagian atau partial acquisition harus dicatat semua informasi yang terkait dengan barang bukti digital seperti, informasi direktori, informasi berkas atau informasi terkait sistem terakuisisi. Adapun hal yang diperkenankan akuisisi sebagian jika dalam kondisi:

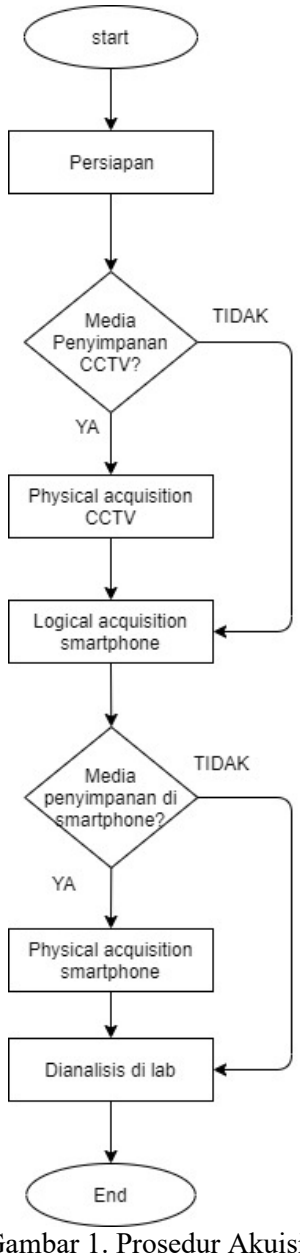
a. Sistem penyimpanan yang terlalu besar sebagai contoh peladen basis data;

b. Sistem tidak boleh mati;
c. Data yang tersalin dimungkinkan bukti digital yang tidak terkait dengan tindak kejahatan;
d. Keterbatasan dengan aturan yang berlaku (Haryadi & Supriyono, 2017).

Dalam tahapan akuisisi yang tercantum di SNI ISO/IEC 27037:2014 diperkenankan melakukan akuisisi secara logikal. Akuisisi secara logikal dilakukan oleh Digital Evidence First Rensponder (DEFR) pada data yang spesifik, direktori atau partisi tertentu. Pada smartphone basis data yang digunakan dalam bentuk SQLite. Untuk smartphone bersistem operasi Android SQLite tersimpan pada direktori /data/data/ (Hariyadi & Huda, 2015).

Dalam penelitian ini mengadopsi ACPO dan Standar Nasional Indonesia (SNI) ISO/IEC 27037:2014 tentang Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital (Badan Standardisasi Nasional 2014). Gambar 1 menjelaskan prosedur akuisisi yang digunakan dalam penelitian. Adapun penjelasannya sebabagai berikut:

a. Persiapan akuisisi merujuk pada penelitian sebelumnya terkait kerangka akuisisi CCTV menggunakan standar ACPO dan SNI ISO/IEC 27037:2014 (Hariyadi et al., 2018).
b. Melakukan pemeriksaan media penyimpan yang terpasang pada smart CCTV.
c. Melakukan akuisisi secara fisik media penyimpan yang terpasang pada smart CCTV.
d. Melakukan akuisisi secara logikal pada ponsel cerdas. Dalam hal ini, melakukan akuisisi pada aplikasi yang terinstal pada smartphone.
e. Memeriksa ketersediaan media penyimpan eksternal pada ponsel cerdas. Jika memiliki media penyimpan eksternal media dilakukan akuisisi fisik.
f. Jika tidak memungkinkan melakukan akuisisi pada Tempat Kejadian Perkara (TKP) maka dilakukan akuisisi di laboratorium forensik. Adapun barang bukti elektronik yang di akuisisi diantaranya: router, access point, smart CCTV, ponsel cerdas, dan media penyimpan.



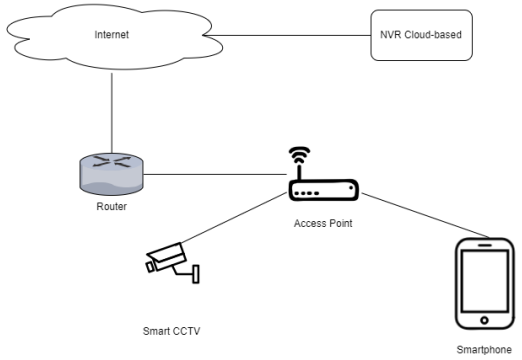
Gambar 1. Prosedur Akuisisi Smart CCTV

Proses akusisi menggunakan metode akuisisi fisikal. Dimana media penyimpanan dengan verifikasi barang bukti baik barang bukti digital, maupun media penggadaannya pun harus sama. Akuisisi Logical akan dilakukan apabila terdapat kondisi kritis, misalnya adalah tidak boleh dimatikannya barangbukti saat proses copy data.

Selaras dengan penelitian Haryadi yang menulis bahwa Proses akuisisi logikal hanya menyalin berkas yang aktif dan artefak lainnya termasuk diantaranya mengakuisisi partisi. (Haryadi & Supriyono, 2017).

4. HASIL DAN PEMBAHASAN

Topologi secara umum pemasangan smart CCTV membutuhkan koneksi internet. Smart CCTV tidak membutuhkan DVR atau NVR yang terinstal secara on-promise melainkan berbasis teknologi komputasi awan. Oleh karena itu mengakses rekaman video pada DVR atau NVR menggunakan aplikasi khusus yang dirancang untuk mengakses DVR atau NVR yang berbasis teknologi komputasi awan. Untuk mengaksesnya dapat menggunakan ponsel cerdas. Gambar 1 menunjukkan topologi pemasangan smart CCTV pada sebuah rumah. Dalam hal ini rumah cerdas.



Gambar 2. Topologi Smart CCTV

Berdasarkan topologi smart CCTV pada rumah cerdas seperti tampak pada Gambar 2 terpasang sebuah smart CCTV merk Xiaomi tipe Xiaofang dan aplikasi yang terinstal pada ponsel cerdas yang bersistem operasi android adalah Mi Home. Berdasarkan prosedur pada Gambar 1 maka barang bukti digital yang didapatkan sebagai berikut:

a. Dua buah *image* hasil akuisisi secara fisik dari media penyimpan yang terpasang pada smart CCTV maupun ponsel cerdas. Hasil *image* telah diverifikasi menggunakan *hash* untuk menjaga integritas barang bukti digital(Kurniawan, 2014).
b. Hasil akuisisi secara logikal pada ponsel cerdas berupa barang bukti digital yang tersimpan pada direktori /data/data/com.xiaomi.smarthome.

5. KESIMPULAN DAN SARAN

a. Kesimpulan

Teknik akuisisi untuk smart cctv menggunakan teknik fisikal dan logikal. Teknik fisikal, membuat *image* dari media penyimpan (*SD Card*) yang terpasang di smart CCTV dan ponsel cerdas. Sedangkan teknik logikal, membuat salinan dari sebuah direktori yang sesuai dengan kaidah forensik digital (Hariyadi & Huda, 2015). Maka menghasilkan tiga barang bukti digital yaitu hasil *image* SD Card smart CCTV, hasil image SD Card ponsel cerdas, dan kumpulan berkas aplikasi Mi Home.

b. Saran

Pada penelitian ini belum melakukan akuisisi dan analisis pada perangkat pendukung seperti router maupun access point. Harapan untuk penelitian berikutnya akuisisi barang bukti lebih difokuskan menggunakan ke perangkat lain yang menghubungkan smartphone dengan smart CCTV serta lebih detail dalam menganalisis barang bukti digital yang tersimpan pada direktori /data/data/com.xiaomi.smarthome.

6. REFERENSI

Asosiasi Penyelenggara Jasa Internet Indonesia, & Teknopreneur. (2018). *Penetrasi & Profil Perilaku Pengguna Internet Indonesia 2017*. Retrieved from www.apjii.or.id

Buzarovska Lazetik, G., & Koshevaliska, O. (2013). Digital evidence in criminal procedures - A comparative approach. *Balkan Social Science Review*, *2*, 63–82.

Danuri, M., & Suharnawi. (2017). Trend Cyber Crime Dan Teknologi. *Infokam*, *2*(September), 55–64.

Davies, T. (2015). Internet of things. *Journal of the Institute of Telecommunications Professionals*, *9*(4), 38. https://doi.org/10.1109/sccs.2019.8852623

Delgado, A.R., Picking, R. & Grout, V. (2006). *Remote-controlled home automation systems with different network technologies. International Network Conference (INC 2006)*.

Gill, M., & Spriggs, A. (2005). *Assessing the impact of CCTV: Home Office Research Study*. (February), 176p.

Hariyadi, D., & Huda, A. A. (2015). Laron: Aplikasi Akuisisi Berbasis SNI 27037:2014 pada Ponsel Android. *Indonesia Security Conference 2015*, (September), 1–10. https://doi.org/10.13140/RG.2.1.3819.9520

International Conference on Informatics for Development, 22–25.

Haryadi, D., & Supriyono, A. R. (2017). Kerangka Investigasi Forensik Pada Peladen Pertukaran Berkas Samba Berdasarkan SNI ISO/IEC 27037:2014. *Telematika*, *14*(01), 62–67. https://doi.org/10.31315/telematika.v14i01.1967

Kurniawan, S. (2014). *Perancangan Prosedur Operasional Standar Penanganan Alat Bukti Digital: Studi Kasus Kementerian Komunikasi dan Informatika*. Universitas Indonesia.

Meutia, E. D. (2015). Internet of Things – KeamanandanPrivasi. *Seminar Nasional Dan Expo TeknikElektro,Pp*.

Nurzeni, N. (2009). *Pemanfaatan Internet di Perpustakaan UIN Sunan Kalijaga Yogyakarta sebagai Sarana Penunjang Proses Pembelajaran Bagi Mahasiswa UIN Sunan Kalijaga Yogyakarta*. Universitas Islam Negeri Sunan Kalijaga Yogyakarta.

Oliver, J. (2013). Analisis Hukum Pidana Islam Terhadap Kekuatan Barang Bukti Rekaman Elektronik Closed Circuit Television (Cctv) Dalam Putusan Tindak Pidana Pencurian (Studi Putusan Nomor. 188/Pid.B/2016/Pn.Plg) (Vol. 53). https://doi.org/10.1017/CBO9781107415324.004

Prabowo, M. Y., Budiyanto, A., Nurcahyani, I., & Adinandra, S. (2018). *Perancangan Prototype Smart Home System dengan Internet of Things*. *2018*(November), 131–141.