BAB I
PENDAHULUAN

1.1 Latar Belakang

Tindak kejahatan dan kriminalitas dengan memanfaatkan kemajuan teknologi digital dan elektronik dengan menggunakan handphone, smartphone, komputer, internet, serta sosial media. Kemajuan teknologi juga dapat membuktikan kejahatan bagi pelaku tindak kriminalitas. Karena tidak ada kejahatan tanpa meninggalkan jejak. Dibutuhkan barang bukti yang sah dan terbukti keasliannya untuk mengungkap kasus, melacak dan, menjerat pelaku tindak kriminalitas. Barang bukti tidak hanya berasal dari alat elektronik dan data yang dipakai oleh pelaku tetapi juga dapat ditemukan pada alat keamanan seperti CCTV (*Closed Circuit* Television) ataupun dari smartphone yang dapat merekam video untuk menunjukkan kejadian kriminalitas[1].

Salah satu tindak kejahatan yang pernah terjadi dengan menggunakan CCTV sebagai barang bukti digital yaitu Kasus Kopi Sianida Jesicca pada tanggal 6 januari 2016 silam yang menjadikan Jesicca kumala wongso sebagai pelaku utama (tersangka) dan Mirna salihin menjadi korban dikarenakan meninggal sesaat setelahC 9 meminum kopi yang dipesan oleh jesicca di Kafe Olivier. Barang bukti yang didapatkan berupa hasil rekaman CCTV yang diekstrak dari CCTV Cafe Olivier kemudian di simpan pada USB Flashdisk, kemudian dilakukannya analisis dengan empat metode yaitu analisis Metadata, *Frame*, Bitrate, dan analisis Hash. dengan melakukan *zooming* pada salah satu *frame* dan melakukan peningkatan gambar yaitu teknik *enhancement* ditemukannya pergerakan *pixel* halus saat jesicca memasukan sesuatu ke kopi yang dipesan untuk mirna. Tanpa di perhatikan dengan teliti serta tidak melakukan teknik *enhancement* pada *frame* pergerakan jesicca sulit untuk terlihat, hal itu yang membuktikan jessica sebagai tersangka pelaku pembunuhan[2].

Contoh lain tindak kejahatan yang menggunakan CCTV sebagai barang bukti yaitu Kasus Pembunuhan Brigadir J (Nofryansah Yosua Hutabarat) yang sampai

saat ini masih dilakukannya penyelidikan siapa dalang pembunuhan tersebut. Dalam kasus tersebut barang bukti berupa beberapa rekaman CCTV di berbagai daerah, Karena durasi rekaman yang sangat panjang sehingga sulit untuk melakukan analisis *localization tampering* yaitu analisis *frame by frame* menghitung histogram dan menampilkan grafik histogram. Cara lain yang dilakukan yaitu dengan analisis sinkronisasi arah dari bayangan jam matahari di beberapa lokasi kejadian dengan time stamp yang berada dalam video. Setelah dilakukanya analisis sinkronisasi arah bayangan matahari ditemukannya kejanggalan yaitu ketidak cocokan time stamp yang berada dalam video dengan simulasi arah bayangan matahari. Hal itu yang membuktikan rekaman video CCTV yang diberikan sebagai barang bukti telah dimanipulasi dan membuktikan bahwa adanya rekayasa dari kejadian yang sebenarnya[3].

Rekaman video merupakan barang bukti digital yang sah yang biasanya akan ditanyakannya keaslian video pada waktu di pengadilan maka dari itu diperlukannya analisis keaslian untuk mendeteksi keaslian dari video yang akan diserahkan karena sebuah *frame* dalam video dapat dirusak maupun diubah dengan software editing yang bertujuan untuk memalsukan ataupun menyelewengkan suatu tindak kriminalitas yang terjadi. Pelaku kriminalitas sering kali mendapatkan keringanan bahkan di bebaskan dari jeratan hukum dikarenakan video sebagai barang bukti sudah tidak bisa digunakan sebab telah dilakukannya manipulasi [12].

Salah satu contoh manipulasi video dapat berupa tindakan mengedit, menambah, menghapus objek maupun elemen-elemen yang berada dalam *frame* dengan software editing contohnya *Adobe After effect* dan *Adobe premiere pro*. Tindakan manipulasi dalam sebuah video masih wajar dilakukan untuk meringkas durasi dengan menghapus banyak scene karena hasil rekaman yang sangat panjang. Namun menjadi tidak wajar jika tujuan manipulasi bukan untuk meringkas durasi melainkan membuang scene tertentu atau menambah dan menghapus objek dalam *frame* karena merupakan elemen-elemen penting dalam video sebagai barang bukti[4].

Dalam penelitian sebelumnya *tampering* dapat berupa tindakan menambahkan objek ataupun gambar yang berupa rangkaian beberapa *frame* video lain baik sama

maupun beda [5] . Klasifikasi deteksi video dapat dibedakan menjadi dua yaitu *localization tampering* dan *tampering detection*. *Localization tampering* merupakan metode yang menunjukan kejanggalan pada *frame* tertentu dengan cara menganalisis *frame by frame* pada video yang telah dimanipulasi. *Tampering detection* merupakan metode yang hanya bisa melakukan pengecekan integritas dari video dan tidak dapat menunjukan letak *frame* video yang telah dimanipulasi.[6]

Dalam penelitian ini akan membahas serta menganalisis perbandingan hasil rekaman video asli dengan video yang telah dilakukan *attack tampering* serta manipulasi yang berasal dari *smartphone*, karena smartphone termasuk alat elektronik yang sudah memiliki kamera dan perekam yang sering digunakan untuk merekam berbagai kejadian berupa video. Video manipulasi serta temperinng yang akan di lakukan adalah mengedit *timestamp* dan *attack tampering* berupa *cropping,zooming,rotation,dan grayscale*. Penerapan manipulasi tersebut termasuk hal yang sering dilakukan di masyarakat karena merupakan hal yang mudah dilakukan. Namun jika tidak dilakukannya analisis pada video akan sulit mendeteksi perubahan yang terjadi dalam video.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas,permasalahan yang akan dibahas dalam penelitian sebagai berikut :

1. Bagaimana cara untuk mendeteksi keaslian video sebagai barang bukti digital?
2. Apakah simulasi bayangan sinar matahari dapat digunakan untuk memverifikasi time stamp yang berada dalam video?
3. Apakah metode *localization tampering* dapat digunakan untuk mendeteksi adanya manipulasi ?

1.3 Batasan Masalah

Berdasarkan rumusan masalah diatas, peneliti memfokuskan pokok pembahasan dalam penelitian ini dengan membatasi ruang lingkup yaitu :

1. File rekaman video berasal dari smartphone merk IPHONE model IPHONE 11.
2. Telah mengetahui format video yang di digunakan oleh media perekam sesuai dengan ketentuan merk dalam penelitian ini menggunakan *smartphone* merk iphone 11.
3. Simulasi rekayasa yang dilakukan pada video yaitu berupa *cropping,zooming,rotation,grayscale*, dan manipulasi *timestamp*.
4. Manipulasi video menggunakan aplikasi yang sudah ada.
5. Hanya mengidentifikasi terjadinya manipulasi pada sebuah video.
6. Pendeteksian manipulasi timestamp menggunakan simulasi bayangan sinar matahari pada rekaman siang hari dengan menggunakan autodesk sketchup.
7. .Pendeteksian file rekaman video menggunakan metode *localization tampering*.
8. Tidak melakukan prosedur forensik pada smartphone merek IPHONE model IPHONE 11.

1.4 Tujuan Penelitian

Tujuan peneliti melakukan penelitian ini sebagai berikut:

1. Mengetahui keaslian video sebagai barang bukti dengan *metode localization tampering* dan simulasi arah bayangan matahari dari hasil rekaman *smartphone* merk iphone 11.
2. Mengetahui apakah simulasi arah bayangan matahari dapat memverifikasi timestamp dalam video hasil rekaman *smartphone* merk iphone 11.
3. Mengetahui apakah metode *localization tampering* dapat mendeteksi keaslian barang bukti digital berupa video hasil rekaman *smartphone* merk iphone 11.

1.5 Metodologi Penelitian

Berdasarkan penelitian kali ini akan dilakukannya metode *localization tampering* yaitu metode untuk mengetahui deteksi pada suatu video yang telah dilakukan manipulasi pada beberapa *frame* dengan mengetahui nilai pixel yang berada dalam video yang telah dilakukannya *attack tampering*, serta melakukan simulasi arah bayangan matahari menggunakan *autodesk sketchup* untuk memverifikasi *timestamp* yang ada dalam video. Langkah-langkah yang akan digunakan untuk menerapkan metode penelitian sebagai berikut :

1. Collection

   Pada langkah ini collection Merupakan langkah kegiatan pengumpulan barang bukti kejahatan digital yang akan dilakukan oleh peneliti yang di peroleh dari *smartphone* merk iphone 11.
2. Examination

   Pada langkah ini examination adalah tahap pemeriksaan meta data yang telah dikumpulkan untuk memastikan data yang diperoleh berupa file asli hasil perekaman *smartphone* merk iphone 11.
3. Analysis

   Pada langkah ini akan dilakukan beberapa analysis dari hasil rekaman *smartphone* merk iphone 11 untuk mendapatkan hasil analisis yang lebih akurat pada file yang telah diperoleh dengan melakukan analysis metadata menggunakan mediainfo, metode *Localization tampering* dan analysis

verifikasi Timestamp menggunakan simulasi bayangan matahari dengan menggunakan Autodesk sketchup.

1.6 Sistemmatika Penulisan

Agar penyajian penulisan penelitian mudah dimengerti dan terstruktur. Maka dibuatlah tahapan-tahapan penulisan yang disusun secara sistematis dengan urutan BAB I sampai dengan BAB V sebagai berikut :

BAB I PENDAHULUAN

Tahapan ini berisikan uraian latar belakang masalah, rumusan masalah , batasan masalah, tujuan penelitian, manfaat penelitian, serta sistematika penulisan yang dilakukan.

BAB II TINJAUAN PUSTAKA

Tahapan ini berisikan uraian tinjauan pustaka yang merupakan hasil review penelitian yang sebelumnya pernah dilakukan dan teori-teori terkait yang dibutuhkan dalam penelitian ini.

BAB III METODE PENELITIAN

Tahapan ini berisikan uraian tentang alat dan bahan yang digunakan dalam penelitian serta menjelaskan alur dari perancangan sebuah penelitian untuk memperoleh hasil akhir dan kesimpulan.

BAB IV HASIL DAN PEMBAHASAN

Tahapan ini berisi uraian hasil akhir dan pembahasan dari penelitian yang telah dilakukan.

BAB V PENUTUP

Tahapan ini berisikan kesimpulan dari seluruh bab sebelumnya dan memberikan saran-saran serta pengembangan untuk penelitian selanjutnya.