TUGAS VI

MATA KULIAH KEAMANAN JARINGAN KOMPUTER

Oleh :

Rofby Hidayadi 09011281020132

Dosen Pengampuh : Deris Stiawan, M.T., Ph.D.

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2018

I. Judul Tugas

Forensik Video dengan Metadata Analisis, Frame Analisis, dan Pixel Analisis

II. Forensik Video

Untuk melakukan simulasi forensik video sederhana ini diperlukan dua video, dimana yang satu merupakan video rekaman asli dan video satunya lagi merupakan video yang sudah mengalami proses editing. Berikut adalah video yang digunakan untuk simulasi forensik video kali ini :

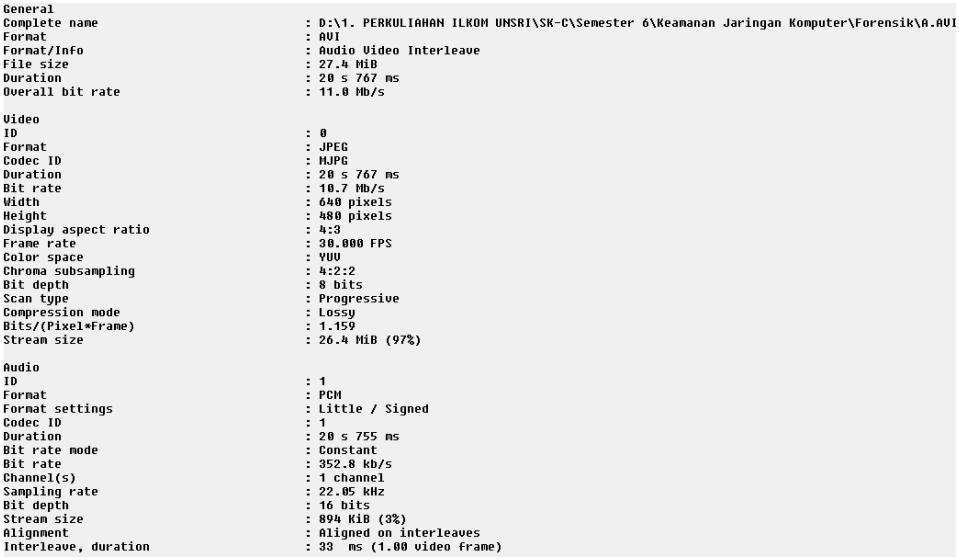
Gambar 1. Video simulasi forensik

Kedua video tersebut kemudian dianalisis berdasarkan metadatanya menggunakan tools MediaInfo (https://mediaarea.net/en/MediaInfo/Download). Kedua video tersebut dapat didownload di https://drive.google.com/open?id=1ffvDp0Tq-yjP_khjmabEBG2vcCjoGqjd. Adapun hasil metadata dari kedua video diatas adalah sebagai berikut :

A. Metadata Analisis

1. Metadata Video A.AVI

   Berikut adalah metadata dari video A.AVI :



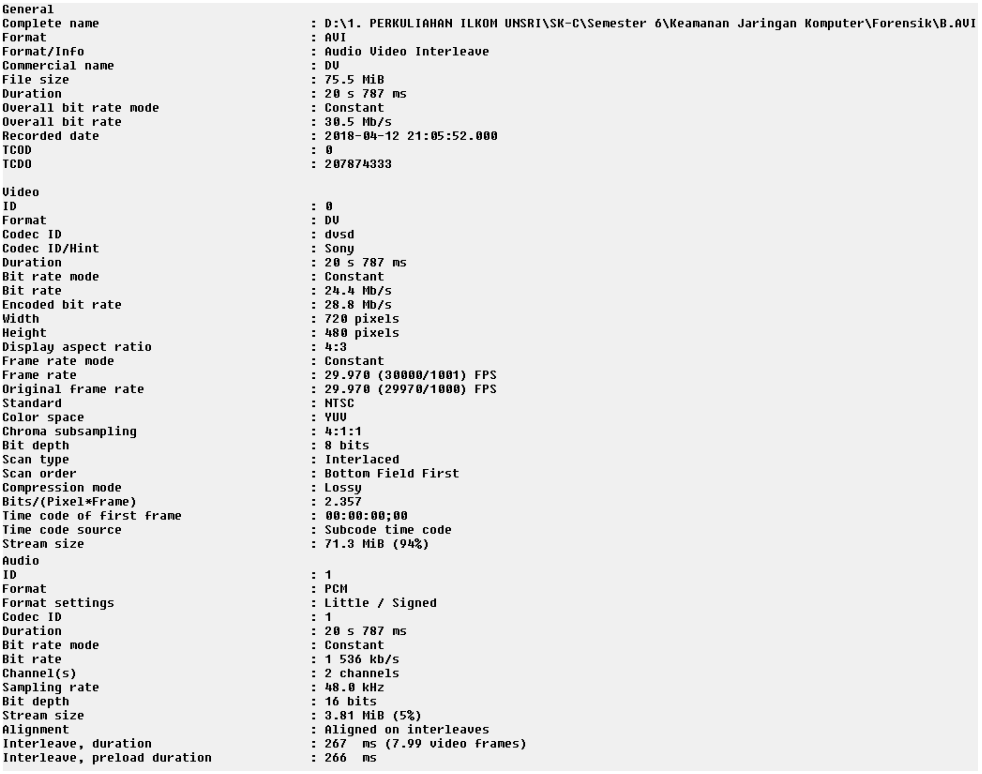
```
General
Complete name                            : D:\1. PERKULIAHAN ILKOM UNSRI\SK-C\Semester 6\Keamanan Jaringan Komputer\Forensik\A.AVI
Format                                   : AVI
Format/Info                              : Audio Video Interleave
File size                                : 27.4 MiB
Duration                                 : 20 s 767 ms
Overall bit rate                         : 11.0 Mb/s

Video
ID                                       : 0
Format                                   : JPEG
Codec ID                                 : MJPG
Duration                                 : 20 s 767 ms
Bit rate                                 : 10.7 Mb/s
Width                                    : 640 pixels
Height                                   : 480 pixels
Display aspect ratio                     : 4:3
Frame rate                               : 30.000 FPS
Color space                              : YUV
Chroma subsampling                       : 4:2:2
Bit depth                                : 8 bits
Scan type                                : Progressive
Compression mode                         : Lossy
Bits/(Pixel*Frame)                       : 1.159
Stream size                              : 26.4 MiB (97%)

Audio
ID                                       : 1
Format                                   : PCM
Format settings                          : Little / Signed
Codec ID                                 : 1
Duration                                 : 20 s 755 ms
Bit rate mode                            : Constant
Bit rate                                 : 352.8 kb/s
Channel(s)                               : 1 channel
Sampling rate                            : 22.05 kHz
Bit depth                                : 16 bits
Stream size                              : 894 KiB (3%)
Alignment                                : Aligned on interleaves
Interleave, duration                     : 33  ms (1.00 video frame)
```

Gambar 2. Metadata video A.AVI

Dari metadata tersebut dapat diketahui bahwa video A.AVI merupakan video rekaman asli. Hal ini dikarenakan pada metadata video tersebut tidak terdapat informasi yang mengindikasikan bahwa video tersebut telah melalui proses editing. Apabila video tersebut telah melalui proses editing, maka akan terdapat informasi tools yang digunakan untuk proses editing.

2. Metadata Video B.AVI

   Berikut adalah metadata dari video B.AVI :



```
General
Complete name                            : D:\1. PERKULIAHAN ILKOM UNSRI\SK-C\Semester 6\Keamanan Jaringan Komputer\Forensik\B.AVI
Format                                   : AVI
Format/Info                              : Audio Video Interleave
Commercial name                          : DV
File size                                : 75.5 MiB
Duration                                 : 20 s 787 ms
Overall bit rate mode                    : Constant
Overall bit rate                         : 30.5 Mb/s
Recorded date                            : 2018-04-12 21:05:52.000
TCOD                                     : 0
TCDO                                     : 207874333

Video
ID                                       : 0
Format                                   : DV
Codec ID                                 : dvsd
Codec ID/Hint                            : Sony
Duration                                 : 20 s 787 ms
Bit rate mode                            : Constant
Bit rate                                 : 24.4 Mb/s
Encoded bit rate                         : 28.8 Mb/s
Width                                    : 720 pixels
Height                                   : 480 pixels
Display aspect ratio                     : 4:3
Frame rate mode                          : Constant
Frame rate                               : 29.970 (30000/1001) FPS
Original frame rate                      : 29.970 (29970/1000) FPS
Standard                                 : NTSC
Color space                              : YUV
Chroma subsampling                       : 4:1:1
Bit depth                                : 8 bits
Scan type                                : Interlaced
Scan order                               : Bottom Field First
Compression mode                         : Lossy
Bits/(Pixel*Frame)                       : 2.357
Time code of first frame                 : 00:00:00;00
Time code source                         : Subcode time code
Stream size                              : 71.3 MiB (94%)
Audio
ID                                       : 1
Format                                   : PCM
Format settings                          : Little / Signed
Codec ID                                 : 1
Duration                                 : 20 s 787 ms
Bit rate mode                            : Constant
Bit rate                                 : 1 536 kb/s
Channel(s)                               : 2 channels
Sampling rate                            : 48.0 kHz
Bit depth                                : 16 bits
Stream size                              : 3.81 MiB (5%)
Alignment                                : Aligned on interleaves
Interleave, duration                     : 267  ms (7.99 video frames)
Interleave, preload duration             : 266  ms
```

Gambar 3. Metadata video B.AVI

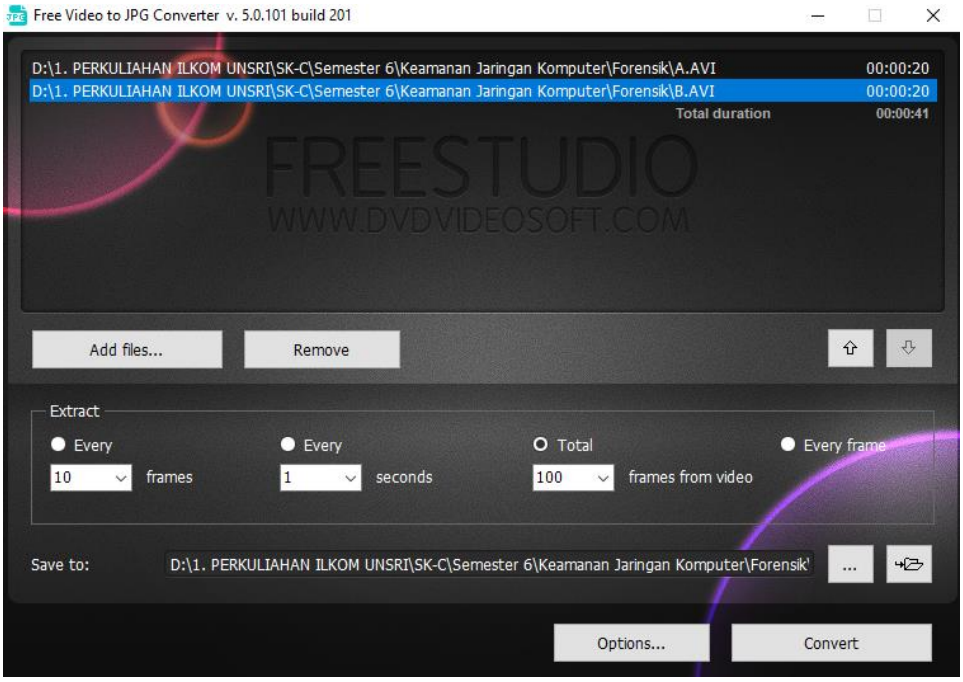
Dari metadata tersebut dapat diketahui bahwa video B.AVI merupakan video yang telah melalui proses editing baik dari segi video ataupun audionya. Hal ini dikarenakan pada metadata video tersebut terdapat informasi bahwa video tersebut telah di editing menggunakan tools dengan vendor Sony. Dalam metadata tersebut juga terdapat informasi bahwa telah terjadi penambahan durasi video selama 20 ms, karena seperti yang diketahui bahwa pada video A.AVI yang merupakan video rekaman asli dengan durasi 20 : 767 ms sedangkan pada video B.AVI yang telah terindikasi merupakan video yang telah diediting durasinya adalah 20 : 787 ms. Dari informasi tersebut, kemungkinan terbesar adalah bahwa video B.AVI telah terjadi penambahan frame.

B. Frame Analisis

Berdasarkan metadata analisis diperoleh kesimpulan bahwa video A.AVI merupakan video rekaman asli, sedangkan video B.AVI merupakan video yang telah diediting dengan indikasi editing adalah penambahan frame. Maka, langkah selanjutnya adalah melakukan frame analisis dengan cara membandingkan frame video A.AVI dengan frame video B.AVI. Hal ini

bertujuan untuk mengetahui letak kejanggalan frame pada video B.AVI yang dicurigai telah terjadi penambahan frame.

Untuk mengubah video menjadi frame, digunakan tools Free Video to JPG Converter (https://www.dvdvideosoft.com/products/dvd/Free-Video-to-JPG-Converter.htm).



Gambar 4. Proses konversi video menjadi frame

Dari gambar 4 dapat diketahui bahwa kedua video akan dikonversi masing-masing menjadi 100 frames. Adapun jumlah frame yang diinginkan dapat disesuaikan dengan kebutuhan, semakin tinggi jumlah frame yang dikonversi maka semakin detail pula video tersebut dapat dianalisis.

Setelah video kedua video dikonversi menjadi frame, didapat kecurigaan pada frames sebagai berikut :

1. Frames video rekaman asli A.AVI 040, 041, 042, 043
2. Frames video yang telah diediting B.AVI 040, 041, 042, 043

Gambar 5. Frame A.AVI 040

Gambar 6. Frame B.AVI 040

Gambar 7. Frame A.AVI 041

Gambar 8. Frame B.AVI 041

Gambar 9. Frame A.AVI 042

Gambar 10. Frame B.AVI 042

Gambar 11. Frame A.AVI 043

Gambar 12. Frame B.AVI 043

Pada frames video rekaman asli A.AVI 040, 041, 042, 043 proses perpindahan frame dari satu frame ke frame yang lainnya berjalan mulus dan teratur. Sedangkan pada frames video yang telah diediting B.AVI 040, 041, 042, 043 proses perpindahan frame dari satu frame ke frame yang lainnya terdapat kejanggalan sebagai berikut :

1. Perpindahan frame B.AVI 040 ke B.AVI 041 tidak halus, jika dibandingkan dengan perpindahan frame A.AVI 040 ke A.AVI 041 maka pada perpindahan frame B.AVI 040 ke B.AVI 041 seperti ada frame yang hilang.
2. Perpindahan frame B.AVI 041 ke B.042 seperti terjadi penumpukan dua frame atau lebih.
3. Jika dibandingkan secara keseluruhan antara frames A.AVI 040, 041, 042, 043 dengan B.AVI 040, 041, 042, 043 terjadi perbedaan frame pada 041,

frame B.AVI 041 merupakan frame A.AVI 042. Hal ini mengindikasikan bahwa frame B.AVI 041 telah terjadi penumpukan frame atau pergantian frame, karena hal ini masih terlihat pada frame B.AVI 042 terlihat sisa penumpukan frame B.AVI 041 ditambah B.AVI 043.

Kesimpulannya adalah kemungkinan besar terjadi penumpukan frame pada video B.AVI tepatnya pada frame B.AVI 041 dan B.AVI 042.

C. Pixel Analisis

Setelah diketahui kemungkinan besar terjadi penumpukan frame pada video B.AVI tepatnya pada frame B.AVI 041 dan B.AVI 042. Maka, langkah selanjutnya adalah melakukan pixel analisis menggunakan metode Error Level Analysis (ELA). Adapun tools yang digunakan adalah tools online yaitu melalui http://fotoforensics.com/. Pada umumnya gambar JPEG menggunakan jenis kompresi lossy, sehingga setiap melakukan resave, kualitas akan semakin berkurang. Algoritma JPEG beroperasi pada 8 x 8 pixel grid, sehingga jika tidak terjadi modifikasi, maka setiap grid memiliki potensi error yang sama hal ini ditunjukkan dengan titik-titik putih pada ELA. Berikut adalah ELA dari frame yang dimaksud :

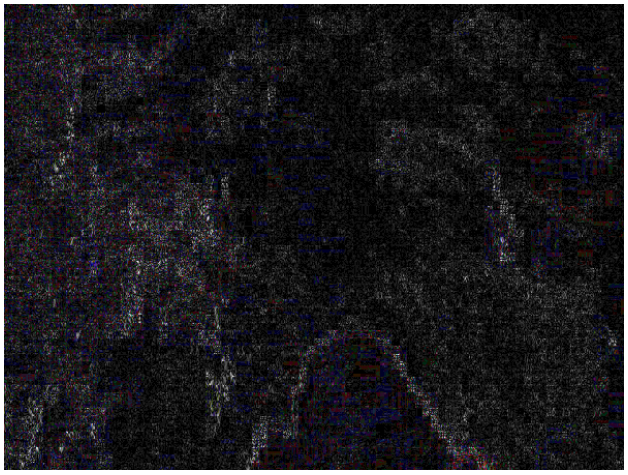
Gambar 13. Frame A.AVI 041

Gambar 14. ELA Frame A.AVI 041

Gambar 15. Frame B.AVI 041

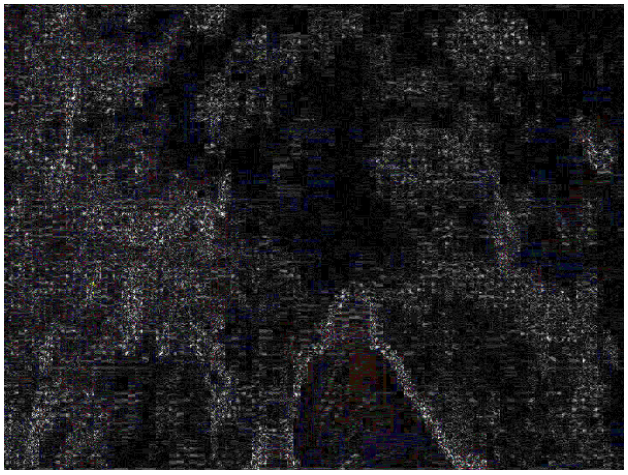
Gambar 16. ELA Frame B.AVI 041

Gambar 17. Frame A.AVI 042



Gambar 18. ELA Frame A.AVI 042

Gambar 19. Frame B.AVI 042



Gambar 20. ELA Frame B.AVI 042

Dari gambar tersebut dapat diketahui bahwa ELA pada frame A.AVI 041 dan 042 adalah normal karena error yang diindikasikan oleh kumpulan titik-titik putih terlihat merata. Sedangkan pada frame B.AVI 041 dan 042 kumpulan titik-titik putih banyak terpusar pada area tertentu yang mengindikasikan bahwa telah terjadi proses editing ataupun penumpukan frame. Semakin banyak kumpulan titik-titik putih yang terpusat pada area tertentu maka hal itu mengindikasikan error yang tinggi pada gambar tersebut. Hal itu berarti bahwa gambar tersebut telah melalui proses editing.

III. Kesimpulan

Adapun kesimpulan pada simulasi kali ini adalah sebagai berikut :

1. Metadata analisis dapt digunakan untuk mengumpukan informasi seperti alat yang digunakan untuk mengambil gambar atau video, ukuran gambar atau video, durasi video, dan lain-lain yang berkaitan dengan informasi lengkap dari gambar atau video tersebut.
2. Pada video selain melakukan metadata analisis, sebaiknya juga melakukan frame analisis dengan melakukan dekompresi video menjadi frames. Frame yang dicurigai kemudian dianalisa dengan metode Error Level Analysis (ELA).
3. Berdasarkan ELA, frame yang diediting akan memiliki penyebaran pixel yang tidak merata atau penumpukan warna tertentu pada sebuah bagian gambar sehingga error levelnya dianggap tinggi.
4. Pada dasarnya video adalah kumpulan dari gambar-gambta berurutan, sehingga saat menganalisa frame dapat dianggap sedang menganalisa sebuah gambar.

IV. Referensi

https://fotoforensics.com/tutorial-ela.php