Nama : Fikri Azmi Naufal

Nim : 1310651148

Kelas : A

Soal I

Access Control

Access Control memiliki tujuan untuk untuk memungkinkan pengguna yang berwenang mengakses data yang sesuai dan menolak akses ke pengguna yang tidak sah. Kontrol akses memiliki manfaat diantaranya melindungi sebuah data dari ancaman seseornag yang tidak memiliki akses, menjaga kerahasiaan dan melindungi file dari seseorang yang tidak berwenang yang ingin memodifikasi file.

Akses Control memiliki beberapa konsep dasar diantaranya :

- *Confidentiality(Kerahasian), integrity, dan availability (Ketersediaan)*

  Confidentiality(Kerahasian) berusaha untuk mencegah pengguna yang tidak sah, sehingga tidak semua pengguna bias mengakses data tersebut. Sedangkan integrity berusaha untuk mencegah seseorang yang tidak berhak memodifikasi data. Availability (Ketersediaan) memastikan bahwa data selalu tersedia kapanpun.
- *Identity and authentication, authorization, and accountability*

  Identity and authentication berarti memverifikasi identitas pengguna yang akan mengakses data. Authorization berarti pengesahan identitas pengguna untuk mengakses data. Sedangkan accountability beararti identitas benar benar bias di pertanggungjawabkan ke asliannya.
- *Nonrepudiation*

  Nonrepudiation maksudnya adalah menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi.
- *Least privilege and need to know*

  Least privilege and need to know maksudnya adalah membatasi jumlah hak akses
- *Subjects and objects*

Sebuah subjek merupakan entitas aktif pada system data, sedangkan object murpakan entitas pasif pada system data.

- *Defense -in-depth*

  Pertahanan berlapis untuk mengurasi resiko.

MODEL ACCESS CONTROL

Model access control terdiri dari Discr etionary access controls , Nond iscretionary access control, Rule-based access controls dan lain lain. Model utama dari model akses control adalah adalah Discretionary Control (DAC), Mandatory Access Control (MAC), dan nondiscretionary access control.

Berikut adalah model dari acces control adalah :

- *Discretionary access controls*

  Discr etionary access controls sistem komputer untuk membatasi akses ke suatu objek berdasarkan identitas atau kelompok yang di miliki. Pada DAC user diklasifikasikan berdasarkan kepemilikan atu kelompok. Contoh : akses ke program aplikasi / database, share resource.

- *Mandat ory access controls*

  Jenis kontrol akses dimana sistem yang memutuskan bagaimana data akan di akses atau di share atau melakukan beberapa jenis operasi pada obyek. Pada MAC user diklasifikasi berdasarkan level dan lebih aman dibanding Discr etionary access controls. MAC akan mengantisipasi Pengaksesan terhadap File yang rahasia.

- *Role-Based Access Control (RBAC)*

  Role-Based Access Control (RBAC) mendefinisikan bagaimana informasi diakses pada sistem berdasarkan peran subjek. RBAC mengacu pada role based security. Dalam organisasi, roles dibuat untuk fungsi kerja yang berbeda. Dengan kata lain peran keanggotaan didasarkan pada kompetensi, tugas, dan kewenangan.

- *Centralized access control*

  Centralized access control atau juga bias disebut Kontrol akses terpusat. Kontrol akses terpusat berkonsentrasi kontrol akses di satu titik logis untuk sistem atau organisasi. Kontrol akses terpusat dapat digunakan untuk menyediakan Single Sign-On (SSO), di mana subjek dapat mengotentikasi sekali, dan kemudian mengakses beberapa sistem.

- *Access contr ol lists*

  merupakan sebuah metode yang digunakan untuk menyeleksi paket-paket yang keluar masuk.

- *User entitlement, access review, and audit*

  Akses agregasi (bergabungnya bagian-bagian yang terpisah) terjadi sebagai pengguna individu memperoleh lebih banyak akses ke banyak sistem.

ACCESS CONTROL DEFENSIVE CATEGORIES AND TYPES

Untuk memahami dan menerapkan kontrol akses, pemahaman setiap kontrol sangat penting untuk dapat menambah keamanan. Pada bagian ini, setiap jenis kontrol akses akan ditentukan atas dasar bagaimana menambah keamanan sistem.

Ada enam jenis kontrol akses:

• Pencegahan
• Detektif
• Corrective
• Pemulihan
• Pencegah
• Kompensasi

AUTHENTICATION METHODS

Proses otentifikasi pada prinsipnya berfungsi sebagai kesempatan pengguna dan pemberi layanan dalam proses pengaksesan resource. Pihak pengguna harus mampu memberikan informasi yang dibutuhkan pemberi layanan untuk berhak mendapatkan resourcenya. Sedang pihak pemberi layanan harus mampu menjamin bahwa pihak yang tidak berhak tidak akan dapat mengakses resource ini.

Metode-Metode Autentikasi :

- Type 1 authentica tion: something you know

  Cara ini mengandalkan kerahasiaan informasi, contohnya adalah password dan PIN. Cara ini berasumsi bahwa tidak ada seorangpun yang mengetahui rahasia itu kecuali anda seorang.

  - Password hashes and password cracking
    - Dictionary attacks
    - Hybrid attacks

- ❖ Brute-force attacks
- ❖ Rainbow tables
- ❖ Salts

- Type 2 authentication: something you have

  Type 2 authentication (sesuatu yang harus kamu punya) meminta user untuk memproses sesuatu. Cara ini biasanya merupakan faktor tambahan untuk membuat autentikasi menjadi lebih aman.

  - Synchronous dynamic token
  - Asynchronous dynamic token

- Type 3 authentica tion: something you are

  Cara ini mengandalkan keunikan bagian-bagian tubuh anda yang tidak mungkin ada pada orang lain seperti sidik jari, suara atau sidik retina. Cara ini berasumsi bahwa bagian tubuh anda seperti sidik jari dan sidik retina, tidak mungkin sama dengan orang lain.

  - ❖ Biometric enrollment and throughput
  - ❖ Accuracy of biometric systems
  - ❖ Types of biometric controls

ACCESS CONTROL TECHNOLOGIES

Ada beberapa teknologi yang digunakan untuk pelaksanaan kontrol akses diantaranya :

- Singl e sign- on

  Single Sign On (SSO) adalah sebuah metode kontrol akses yang memungkinkan sebuah user untuk login sekali dan mendapatkan akses ke sistem-sistem perangkat lunak yang berbeda tanpa harus login kembali. SSO menggunakan server otentikasi terpusat dimana semua sistem dan aplikasi menggunakan server tersebut untuk tujuan otentikasi (proses validasi user).

- Federat ed identity management

  FIdM dapat menggunakan OpenID atau SAML (Security Association Markup Language).

- Kerberos

Kerberos adalah layanan otentikasi pihak ketiga yang dapat digunakan untuk mendukung Single Sign-O. Kerberos menggunakan enkripsi simetris dan memberikan saling otentikasi kedua klien dan server.

Kerberos memiliki komponen-komponen berikut :

- Principal: Client (user) atau layanan
- Realm: Sebuah jaringan Kerberos logis
- Ticket: Data yang mengotentikasi identitas kepala sekolah
- credensial: A tiket dan kunci layanan
- KDC: Key Distribution Center, yang mengotentikasi kepala sekolah
- TGS: Layanan Tiket-Pemberian
- TGT: Tiket-Pemberian Tiket
- C / S: Client / Server, tentang komunikasi antara dua

- Sesame

SESAME adalah Sistem Eropa Aman untuk Aplikasi dalam lingkungan multivendor ment, sistem single sign-on yang mendukung lingkungan yang heterogen. SESAME menggunakan Privilege Atribut Sertifikat (PAC)

Soal II.

Menggabungkan beberapa video dengan menggunakan hj-slipt

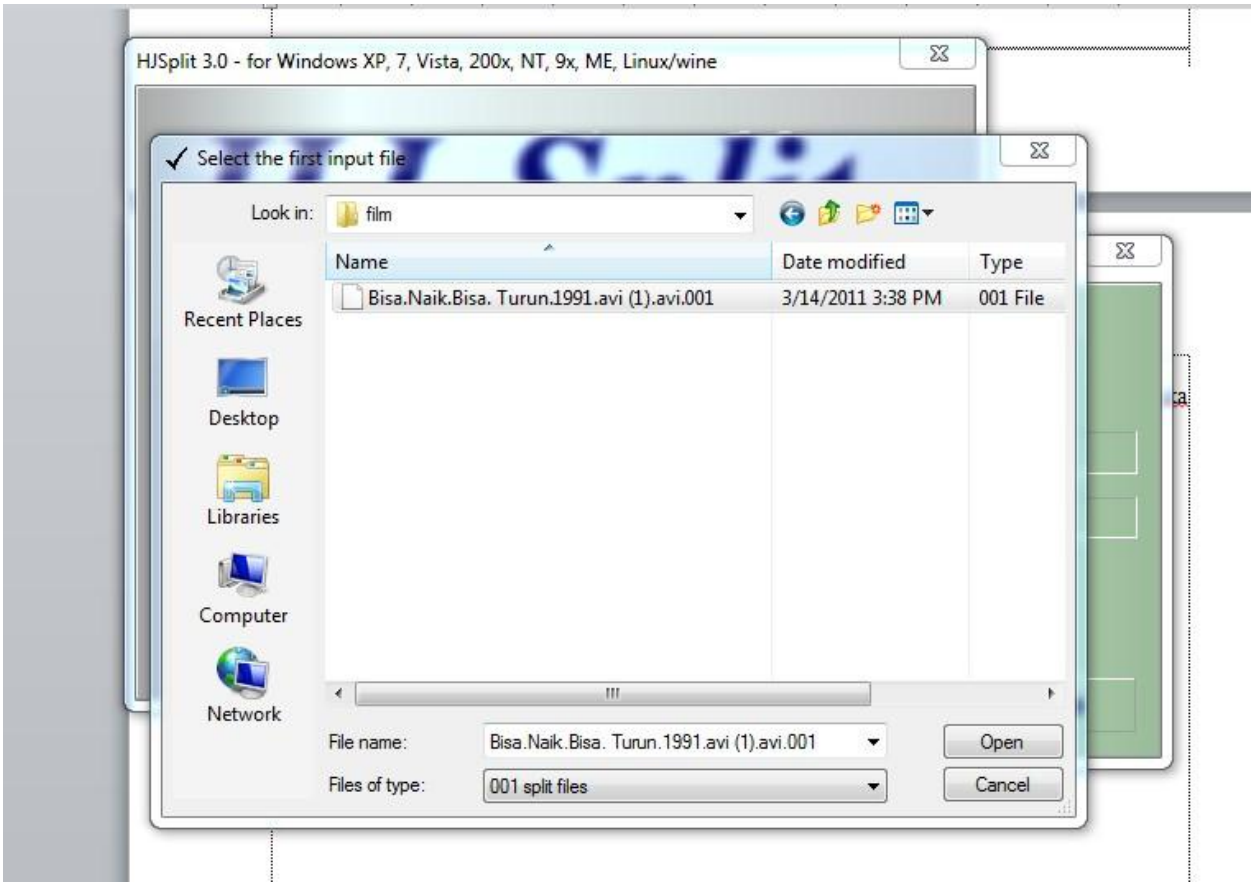
Pertama buka hj-slipt

Klik menu join dan cari dimana anda meletakkan file film yang tersimpan.

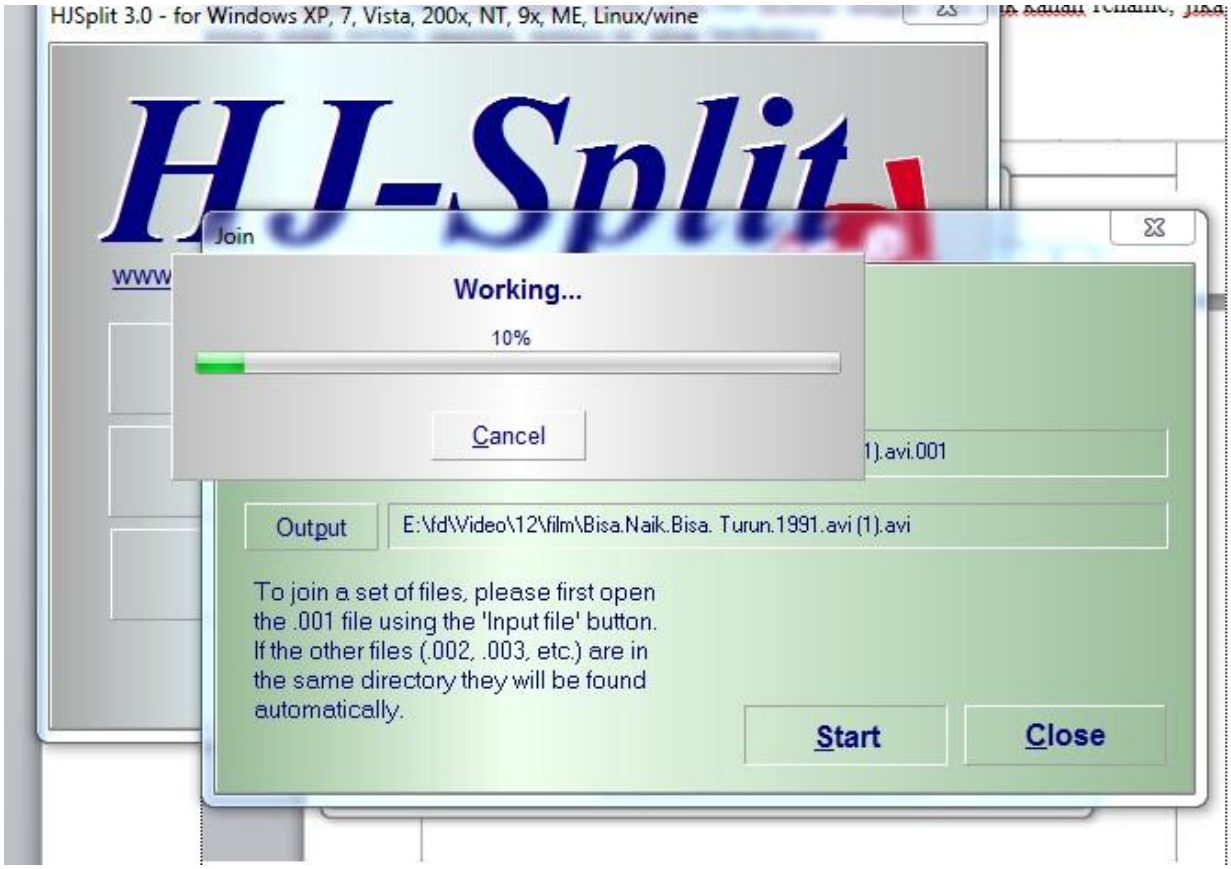
Di sini hanya akan terlihat satu file saja yakni *nama_file.avi.001* , tetapi pada kenyataannya beberapa file. Pastikan ke semua file tersebut sudah memiliki nama yang sama namun ekstensi file tersebut urut, contohnya:

Bisa.Naik.Bisa. Turun.1991.avi (1).avi.001,Bisa.Naik.Bisa. Turun.1991.avi (1).avi.002. Jika terdapat nama file yang tidak sama, rubah nama file tersebut dengan cara klik kanan rename, jika semua sudah normal langsung menuju ke tahap berikutnya

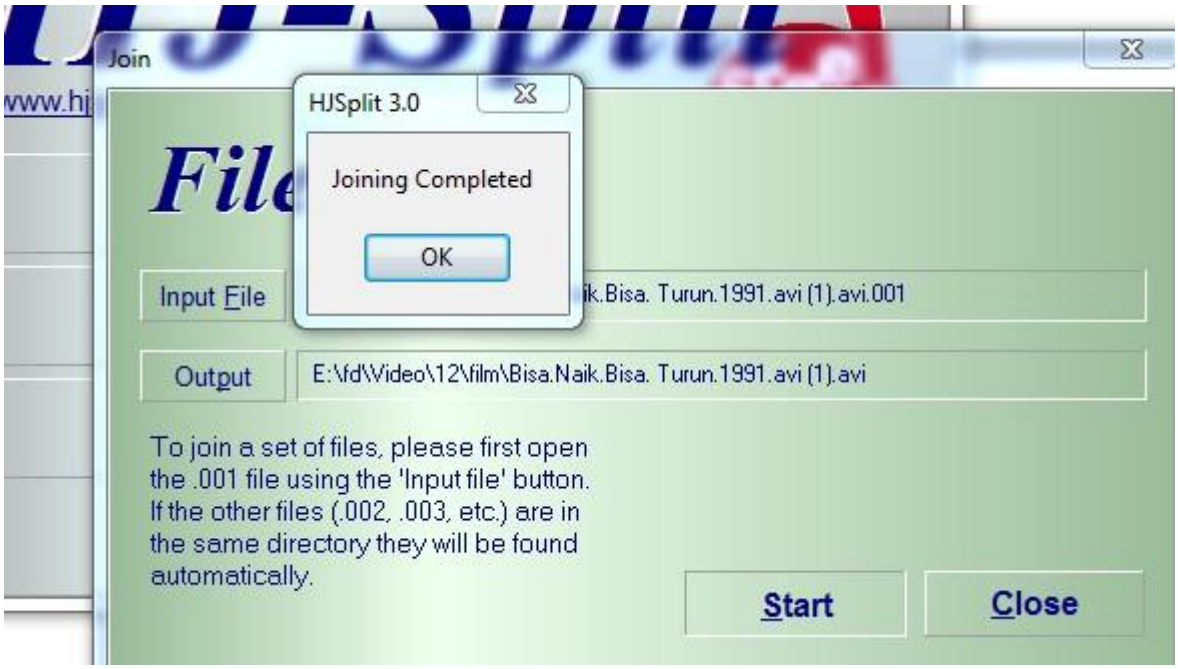
.



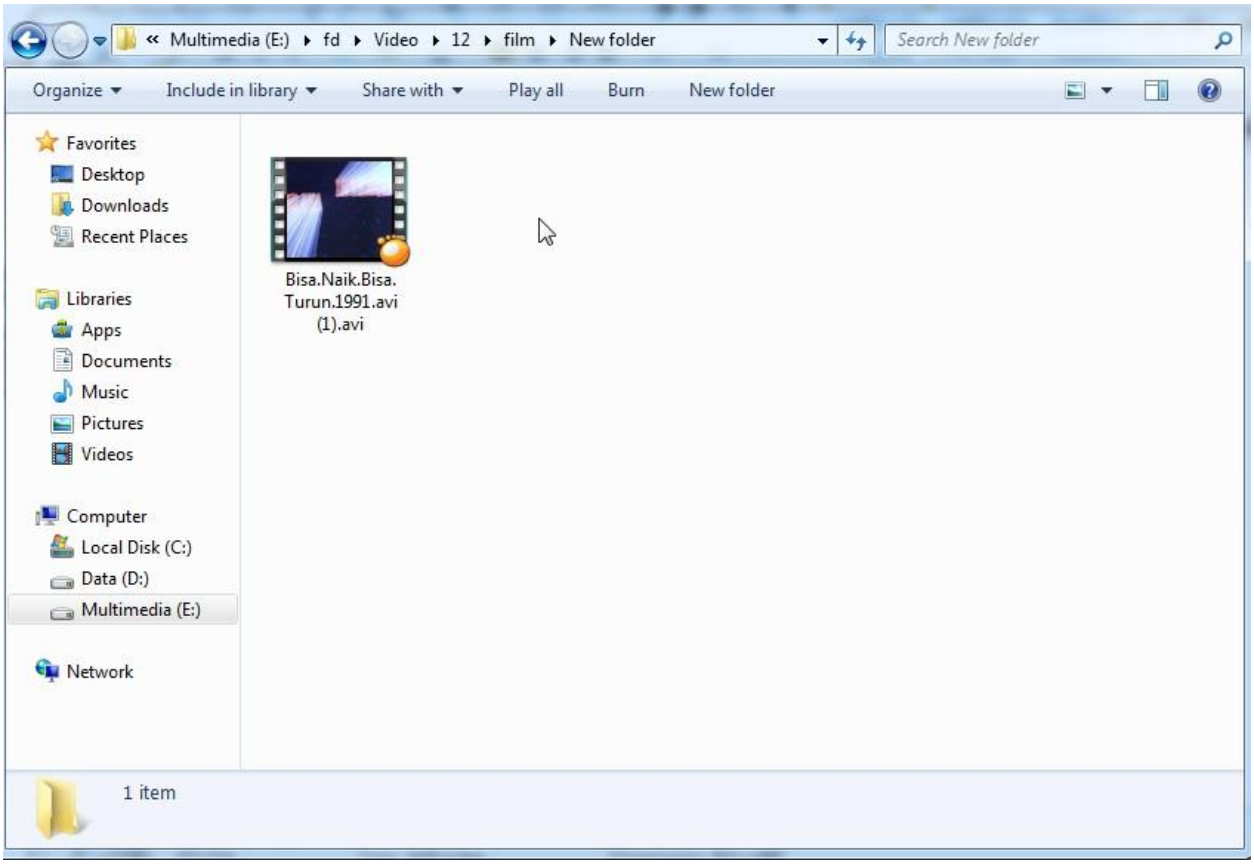
Kemudian kilik start dan tunggu hingga proses penggabungan selesai.



Setelah Proses Selesai



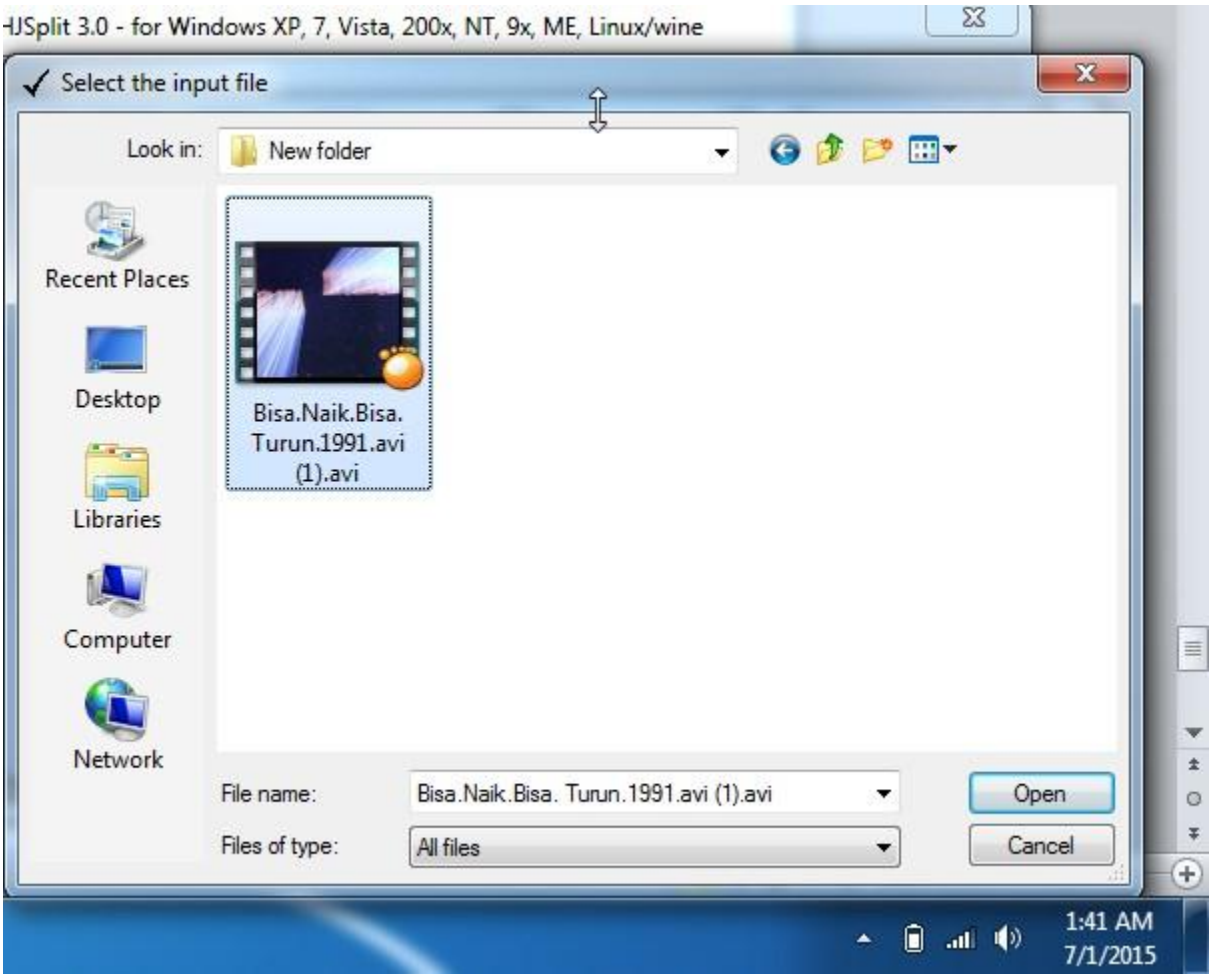
Maka hasilnya



Cara Memecah File Film Menggunakan HJ-Split:

Pertama kita buka HJ-Split kemudian klik split

Klik Input file dan cari dimana anda menyimpan sebuah film yang masih utuh.



Kemudian Klik Open

Maka hasilnya akan tampak seperti di bawah ini