# PROTOKOL DIGITAL SIGNATURE UNTUK MEKANISME PELACAKAN PEMBAJAKAN HAK CIPTA DATA DIGITAL

Rizal Panji Islami (13510066)
*Program Studi Teknik Informatika*
*Sekolah Teknik Elektro dan Informatika*
*Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia*
*rizalpanjiislami@gmail.com*

***Abstrak*—Seiring dengan perkembangan zaman, teknologi informasi semakin berkembang dengan pesat. Didukung dengan berbagai penemuan perangkat pendukung informasi (lebih dikenal dengan sebutan perangkat IT), membuat informasi semakin mudah untuk diakses oleh semua kalangan. Perubahan ini disebut juga dengan digitalisasi informasi. Sebagai dampak dari perubahan radikal atas teknologi informasi ini, banyak perusahaan penyedia konten seperti musik, film, buku, serta berbagai konten lainnya yang pada awalnya menjual konten mereka dalam bentuk fisik, kini mulai beralih ke konten dalam bentuk digital. Konten dalam bentuk digital memiliki berbagai keunggulan, baik ditinjau dari segi lingkungan yang mengurangi emisi sampah, ataupun dari segi biaya produksi yang jauh lebih murah serta transmisi/pengiriman konten yang juga mudah. Sayangnya, berbagai kemudahan yang terjadi sebagai dampak dari digitalisasi bertolak belakang dengan faktor keamanannya, terutama jika ditinjau dari segi perlindungan hak cipta atas konten kekayaan intelektual digital tersebut. Dalam tulisan kali ini penulis mencoba mengusulkan sebuah protokol baru yang dapat digunakan untuk melindungi hak cipta konten digital dengan cara pemberian digital signature. Diharapkan dengan mekanisme protokol baru ini, pembajakan konten digital dapat berkurang.**

***Kata Kunci*—konten digital, pembajakan, protokol, *digital signature***

## I. PENDAHULUAN

Seiring dengan perkembangan zaman, berbagai perangkat dan media yang terkait dengan teknologi informasi saat ini semakin memasyarakat. Saat ini, masyarakat dari berbagai kalangan sudah terbiasa menggunakan berbagai perangkat yang terkait dengan teknologi informasi, seperti dengan komputer, handphone, ataupun tablet. Sebagai dampak dari hal tersebut, berbagai perusahaan yang menyediakan konten terkait dengan kekayaan intelektual, seperti musik, film, buku serta konten-konten lainnya mulai menyediakan berbagai produknya dalam bentuk digital. Terdapat berbagai keuntungan yang terjadi dengan penyediaan berbagai konten dalam bentuk digital ini, baik ditinjau dari segi lingkungan yang mengurangi emisi sampah, ataupun dari segi biaya produksi yang jauh lebih murah serta transmisi/pengiriman konten yang juga mudah.

Sayangnya, berbagai kemudahan yang terjadi sebagai dampak dari digitalisasi bertolak belakang dengan faktor keamanannya, terutama jika ditinjau dari segi perlindungan hak cipta atas konten kekayaan intelektual digital tersebut. Berbagai konten dalam bentuk digital saat ini dapat dengan mudah di-copy dan disebarluaskan dengan berbagai media, seperti flashdisk, CD, ataupun internet. Jika kita telusuri di internet, berbagai konten yang seharusnya adalah konten kekayaan intelektual dari pemilik konten tersebut, tersebar begitu saja dan dapat dengan mudah diunduh serta disebarkan kembali.

Berbeda dengan konten dalam bentuk fisik, konten dalam bentuk digital sangat sulit untuk dilacak asal usul serta siapa yang menyebarkannya. Untuk dapat melindungi hak cipta konten digital, dalam proposal kali ini penulis mengajukan sebuah usulan untuk melakukan mekanisme perlindungan terhadap konten digital. Perlindungan yang dimaksud disini adalah perlindungan dengan memberikan digital signature terhadap berbagai konten digital yang akan disebar ke konsumen. Digital signature yang diberikan akan dilakukan dengan menggunakan protokol khusus yang akan penulis rancang sehingga memungkinkan dilakukan pelacakan terhadap penyebaran konten digital yang terjadi secara ilegal. Selain itu, protokol ini juga memungkinkan untuk mencegah distribusi konten secara ilegal ataupun modifikasi perubahan isi konten dengan memanfaatkan sifat-sifat dari digital signature. Setiap perubahan dari isi konten dapat diketahui, sehingga orisinalitas konten dapat tetap terjaga.

Pembentukan digital signature ini akan dihubungkan dengan berbagai data terkait dengan konsumen pembeli konten digital tersebut, seperti IP, nama, dan data-data lainnya yang dianggap dapat digunakan untuk autentikasi kepemilikan data. Pelacakan dari pembajakan dapat dilakukan dengan menggunakan sistem yang akan penulis rancang sehingga dapat diketahui siapakah pelaku yang melakukan penyebaran konten digital serta bagaimana untuk mencegahnya.

## II. KONTEN DIGITAL

Konten digital atau data digital secara harfiah dapat diterjemahkan sebagai sebuah data yang direpresentasikan dalam bentuk biner (bit-bit data). Data atau konten digital ini hanya dapat diakses dengan menggunakan perangkat khusus yang mampu menerjemahkan bit-bit data tersebut menjadi sebuah informasi yang bermakna. Perangkat tersebut dikenal juga dengan perangkat IT, baik yang bersifat statis ataupun portabel.

Gambar 1
Ilustrasi Konten Digital
(Sumber : http://images.forbes.com)

Konten digital yang saat ini banyak diperjualbelikan secara umum dapat terbagi menjadi konten berupa *ebook*, file musik, file film, serta program atau *software*. Konten-konten tersebut tersedia dalam berbagai tipe data, seperti pdf, mp3, wav, mov, avi, exe, ipa, jar, dan sebagainya. Setiap konten digital pada umumnya memerlukan sebuah aplikasi khusus yang harus digunakan untuk dapat membuka konten tersebut, seperti PDF Reader ataupun Media Player.

Konten digital saat ini diperjualbelikan umumnya dengan menggunakan media internet. Seorang pembeli dapat menghubungi penjual konten melalui internet, lalu jika transaksi sudah disetujui, pengguna tersebut dapat langsung mengunduh konten. Sayangnya, pasca proses transaksi ini, tidak banyak hal yang dapat dilakukan oleh penjual ataupun pembuat konten untuk melindungi konten mereka. Berbeda dengan konten dalam bentuk fisik yang sulit untuk direplika atau dibuat ulang, konten dalam bentuk digital dapat dengan mudah didistribusikan kembali oleh sang pemilik konten. Hal ini dimungkinkan untuk terjadi karena redistribusi konten cukup dilakukan dengan melakukan penyalinan (*copy*) atas bit-bit data dari konten tersebut.

Terdapat beberapa produsen konten digital yang melakukan proteksi terhadap konten yang mereka perjualbelikan tersebut. Bentuk proteksi tersebut pada umumnya dengan melakukan pencegahan (*blocking*) terhadap upaya *copy-paste* konten digital mereka. Namun sayangnya, hal ini menimbulkan berbagai keluhan dari konsumen. Seperti yang diketahui terdapat berbagai media yang dapat digunakan untuk mengakses suatu konten digital, dan pada umumnya seorang konsumen memiliki berbagai media yang berbeda (tidak hanya satu media saja). Selain itu, terdapat peluang konsumen melakukan perubahan bentuk media (pergantian *device*, *upgrade* dan semacamnya) serta kebutuhan konsumen untuk melakukan *backup* terhadap data mereka. Pemberian *blocking* terhadap *copy-paste* konten digital berdampak pada kesulitan atau bahkan kemustahilan untuk melakukan segala proses tersebut bagi seorang konsumen. Kontradiksinya, jika perlakuan *blocking* tidak diterapkan, seorang konsumen yang tidak bertanggungjawab dapat dengan mudah melakukan - redistribusi data tanpa izin dari produsen.

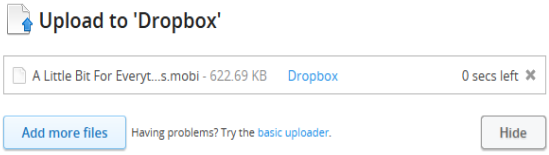
## III. MEKANISME PEMBAJAKAN

Seperti yang sudah dibahas dalam bagian sebelumnya, pada umumnya konten digital didistribusikan melalui media internet. Hal ini membuat mudahnya bagi pemilik konten untuk melakukan redistribusi data secara ilegal atau lebih dikenal dengan istilah pembajakan. Secara umum mekanisme pembajakan terhadap suatu konten digital terjadi seperti berikut:

1. Seorang konsumen yang tidak bertanggungjawab melakukan pembelian (*purchase*) konten di internet, misalkan konten tersebut adalah *ebook* yang dijual di website Amazon.com. Misalkan dalam uji coba kali ini penulis mencoba membeli sebuah *ebook* promo di website Amazon berjudul "A Little Bit of Everything For Dummies" seharga $0.00.
2. Pasca *purchase item* berhasil, penulis dapat mengunduh buku tersebut dalam format .mobi yang merupakan sebuah format khusus untuk device Kindle.


Gambar 2
File .mobi yang Diperoleh

3. Sebenarnya file .mobi ini merupakan sebuah file tersembunyi dalam aplikasi Kindle, namun dengan sebuah aplikasi sederhana (seperti iExplorer) penulis dapat memperoleh file tersebut.
4. Pasca perolehan file .mobi ini, penulis dapat dengan mudah melakukan redistribusi file tersebut melalui media internet. Misalkan dalam uji coba kali ini penulis mengunggah file .mobi tersebut di salah satu website *sharing* data bernama Dropbox.




Gambar 3
Proses Upload Konten di Dropbox

5. Pasca pengunggahan, penulis dapat dengan bebas menjual kembali file tersebut ataupun memberikan kesempatan unduh secara gratis bagi siapapun yang menginginkan file tersebut tanpa pernah dapat dicegah secara langsung oleh penjual konten yang dalam hal ini adalah Amazon.

Dari percobaan yang telah penulis lakukan ini, dapat disimpulkan bahwa proses pembajakan suatu konten digital dapat dilakukan dengan mudah tanpa dapat diawasi secara langsung oleh produsen ataupun penjual konten tersebut.

## IV. DIGITAL SIGNATURE

Sedikit menyinggung mengenai topik lain yang akan berguna dalam proses perlindungan hak cipta digital adalah mengenai *digital siganture*. *Digital signature* atau disebut juga tanda tangan digital merupakan sebuah identitas khusus dari suatu berkas file ataupun teks yang diberikan secara digital melalui sebuah algoritma khusus. Algoritma yang umum digunakan untuk pemberian *digital signature* adalah algoritma DSS (*Digital Signature Standard*).

Dengan pemberian *digital signature* ini, sebuah konten digital dapat diawasi kevalidannya. Seperti yang diketahui, *digital siganture* umumnya dibentuk dengan menggunakan mekanisme perhitungan fungsi SHA yang sangat sensitif terhadap perubahan isi file sekecil apapun. Hal ini akan sangat bermanfaat jika digunakan untuk melakukan perlindungan terhadap konten digital dari pembajakan secara ilegal.

## V. RANCANGAN PROTOKOL PERLINDUNGAN KONTEN DIGITAL

Berangkat dari berbagai permasalahan diatas, penulis pada kesempatan kali ini mencoba untuk merancang sebuah mekanisme atau protokol baru yang dapat digunakan untuk melindungi konten digital serta melacak proses pembajakan yang terjadi. Secara umum protokol ini akan bekerja sebagai berikut:

1. Penyedia konten digital (pihak produsen atau pihak penjual) terlebih dahulu haruslah mendaftarkan diri ke sistem protokol ini, disertai mengunggah konten digital yang akan mereka jual.
2. Setiap pembelian konten digital yang dilakukan oleh konsumen, pihak penjual akan melakukan penjualan tersebut melalui website dari protokol ini.
3. Seorang konsumen yang ingin membeli konten digital melalui sistem ini juga diharuskan untuk membuat sebuah akun khusus.
4. Ketika seorang konsumen ingin membeli suatu konten, konsumen tersebut haruslah memasukkan beberapa data berdasarkan form khusus yang disediakan.
5. Jika dimungkinkan, sistem secara otomatis akan mendeteksi lokasi pembelian dari konten tersebut dan mencatatnya dalam sistem.
6. Sistem akan melakukan *generate* atas digitial signature yang ada dan secara otomatis memasukkannya ke dalam file digital yang akan dibeli oleh konsumen tersebut.
7. Jika seorang konsumen ingin melakukan penyalinan konten, penyalinan tersebut haruslah dilakukan melalui sistem (akan dijelaskan lebih lanjut pada bagian selanjutnya).
8. Ketika terjadi dugaan pembajakan konten, pihak produsen atau penjual konten dapat menganalisa file yang dibajak tersebut melalui sistem ini, sehingga dapat diketahui siapa pelaku pembajakan tersebut. Begitu juga jika penjual konten mencurigai adanya file yang dirubah isinya sehingga isi file tersebut menjadi tidak valid lagi.

Sebagai penjelasan lebih lanjut dari mekanisme diatas, berikut penulis uraikan beberapa analisa dan pertimbangan yang penulis lakukan dalam penentuan mekanisme bagi protokol ini:

1. Registrasi Bagi Pihak Produsen dan Penjual

   Mekanisme awal dari protokol ini adalah setiap produsen konten digital ataupun penjualnya diwajibkan untuk melakukan registrasi ke dalam sistem. Mekanisme ini didesain agar setiap produsen dan penjual dapat melakukan pelacakan terhadap konten yang mereka distribusikan, dan juga demi menjamin autentikasi produsen serta penjual tersebut.

2. Setiap Konten yang Akan Dijual Diunggah ke Dalam Sistem

   Mekanisme berikutnya yang diwajibkan adalah setiap konten yang akan didistribusikan dan ingin dilibatkan dalam sistem ini haruslah terlebih dahulu diunggah dan didaftarkan ke dalam sistem oleh pihak produsen atau penjual. Mekanisme ini dimaksudkan agar sistem dapat menangani konten secara langsung setiap kali produsen atau penjual akan melakukan transaksi penjualan konten tersebut. Selain itu, akses langsung terhadap konten juga dibutuhkan sistem untuk melakukan pemberian *digital signature* terhadap konten tersebut.

3. Konsumen yang Ingin Membeli Haruslah Melakukan Registrasi ke Dalam Sistem

   Setiap konsumen yang ingin membeli konten digital melalui sistem ini diwajibkan untuk melakukan registrasi ke dalam sistem. Hal ini dilakukan agar sistem dapat mengenali konsumen tersebut serta demi mendukung proses pemberial *digital signature* atas konten yang dibeli oleh konsumen tersebut. Mekanisme ini juga diberikan untuk mendukung aktivitas lain dari konsumen yang akan dibahas pada bagian selanjutnya.

4. Penjualan Konten Dilakukan Melalui Sistem

   Setiap pembelian konten yang dilakukan oleh konsumen, pihak produsen atau penjual haruslah melakukan transaksi penjualan tersebut melalui sistem ini. Hal ini dimaksudkan agar sistem dapat

melakukan pemberian *digital signature* yang khusus bagi konsumen tersebut.

5. Pendeteksian Lokasi Konsumen

   Jika dimungkinkan, seandainya perangkat yang digunakan oleh konsumen tersebut memiliki fitur GPS (*Global Positioning Service*), sistem akan melakukan deteksi terhadap lokasi dari konsumen saat melakukan pembelian konten. Lokasi tersebut akan dicatat dalam bentuk *latitude* dan *longitude* dan turut berperan dalam mekanisme pembentukan *digital signature*.

6. Pembentukan Digital Signature Terhadap Seluruh Konten yang Dibeli

   Setiap kali seorang konsumen melakukan pembelian konten, sistem secara otomatis akan melakukan pembuatan *digital signature* berdasarkan data yang diperoleh dan memasukkannya ke dalam sistem. Mekanisme ini merupakan mekanisme utama dari sistem ini, karena dengan metode inilah proses perlindungan konten dapat dilakukan.

7. Proses Penyalinan Melalui Sistem

   Jika seorang konsumen ingin melakukan penyalinan terhadap konten digital yang dimilikinya, penyalinan tersebut haruslah dilakukan melalui sistem. Ketika seorang produsen atau penjual mendaftarkan suatu konten melalui sistem ini, produsen atau penjual tersebut dapat memilih untuk melakukan *copy protection* terhadap file yang mereka miliki. Hal ini membuat file tersebut tidak dapat untuk disalin secara sembarangan.

   Jika seorang konsumen ingin melakukan penyalinan konten ke perangkat yang lain ataupun sekedar melakukan *backup*, konsumen tersebut dapat melakukan proses tersebut melalui sistem ini. Setiap proses penyalinan akan memberikan sebuah digital signature baru atas nama konsumen tersebut.

   Mekanisme ini juga memungkinkan seorang produsen ataupun penjual untuk menentukan berapa kali suatu konten dapat di-*copy* oleh konsumen (seandainya hal tersebut diperlukan).

8. Prosedur Menghadapi Pembajakan

   Dalam pengembangan kali ini sistem tidak mampu untuk mendeteksi secara otomatis apabila terjadi distribusi ilegal dari suatu konten. Namun, jika seorang produsen ataupun penjual menemukan konten mereka didistribusikan secara ilegal, produsen atau penjual tersebut dapat memanfaatkan sistem ini untuk melakukan pelacakan siapakah pemilik dari konten tersebut. Selain itu, produsen dan penjual juga dapat mengetahui apakah suatu konten telah mengalami modifikasi, sehingga kevalidan data dapat tetap terjaga. Hal ini sangatlah penting, terutama jika konten yang didistribusikan berada dalam bentuk *editable* (dapat dimodifikasi kembali).

## VI. RANCANGAN DAN IMPLEMENTASI SISTEM

Sistem ini dirancang untuk bekerja dengan berbasiskan webapp sehingga dapat diakses oleh siapa saja dan dimana saja. Sistem ini diimplementasikan dengan menggunakan bahasa pemrograman PHP dan Java.

1. Rancangan Dasar Sistem

   Fitur dasar dari sistem ini adalah fasilitas registrasi dan login yang dilakukan untuk produsen serta konsumen. Untuk produsen, saat registrasi sistem akan mencatat beberapa data sebagai berikut:

| | |
|---|---|
| Nama Perusahaan | Data ini berupa nama resmi perusahaan, digunakan untuk mencegah duplikasi akun perusahaan dalam sistem |
| Nama Penanggung Jawab | Data ini berupa nama penanggung jawab atau perwakilan perusahaan yang bertugas menggunakan sistem ini |
| Alamat Perusahaan | Data ini merupakan alamat resmi perusahaan yang berguna untuk proses autentikasi kevalidan perusahaan |
| Alamat Email Perusahaan | Data ini merupakan alamat email perusahaan yang menjadi sarana komunikai resmi |
| Alamat Email Penanggung Jawab | Data ini merupakan email dari penanggung jawab |
| Jenis Perusahaan | Data ini merupakan data berupa jenis perusahaan |

Sementara untuk konsumen, data yang akan dicatat adalah sebagai berikut:

| | |
|---|---|
| Nama | Data ini merupakan nama lengkap dari konsumen |
| Email | Data ini merupakan email konsumen yang akan divalidasi oleh sistem |
| Alamat | Data ini merupakan alamat lengkap konsumen (termasuk |

| | |
|---|---|
| | kota dan negara) |
| Metode Pembayaran | Data ini merupakan data berupa metode pembayaran yang akan digunakan oleh konsumen saat melakukan pembelian produk/konten |

Setiap registrasi yang dilakukan oleh produsen dan konsumen secara otomatis sistem akan memberikan sebuah kode (ID) khusus kepada masing-masing produsen dan konsumen tersebut. ID ini akan sangat berguna saat melakukan proses lebih lanjut dalam sistem. Selain itu, setiap produsen akan memperoleh *private key* dan *public key* khusus yang dapat mereka gunakan untuk proses pada *digital signature* nanti.

2. Rancangan Fitur Pendaftaran Konten

Fitur selanjutnya yang tersedia dalam sistem ini adalah fitur pendaftaran konten. Setiap produsen atau penjual yang ingin menjual konten mereka melalui sistem ini haruslah mendaftarkan konten mereka ke dalam sistem. Pendaftaran konten sistem akan mencatat beberapa hal sebagai berikut:

| | |
|---|---|
| Nama Produk | Data ini merupakan nama resmi dari produk yang akan divalidasi oleh sistem demi mencegah duplikasi |
| Harga Produk | Data ini merupakan harga produk yang akan dijual yang sewaktu-waktu dapat dirubah kembali |
| Jenis Lisensi | Data ini merupakan data berupa jenis lisensi dari produk |
| Copy Protection | Data ini berupa pilihan untuk memberikan *copy protection* ke konten tersebut |
| Jumlah Copy | Data ini merupakan data yang dapat dimasukkan oleh produsen jika mereka memutuskan untuk memberikan *copy protection* terhadap produk/konten mereka. Jumlah *copy* adalah berapa banyak seorang konsumen dapat melakukan penyalinan konten dengan menggunakan sistem ini (penjelasan lebih lanjut akan dibahas kemudian) |
| Pengaturan Signature | Data ini merupakan pilihan untuk pengaturan *digital signature* yang akan diberikan ke dalam konten, jika tidak ada pengaturan khusus, isinya akan diset secara *default* |
| Upload Produk | Data ini berupa produk yang didaftarkan dan diupload oleh produsen |

Setiap konten yang didaftarkan oleh produsen secara otomatis akan diberikan kode konten khusus oleh sistem. Kode ini yang dianggap *key* utama pembeda suatu konten dengan konten yang lain.


*Gambar 4*
*Tampilan Fitur Pendaftaran Konten*

3. Rancangan Fitur Pembelian Konten

Fitur selanjutnya yang tersedia adalah fitur pembelian konten yang dapat diakses oleh konsumen. Saat pembelian konten dilakukan pencatatan untuk data-data sebagai berikut:

| | |
|---|---|
| Kode Produk | Data ini diisi oleh sistem secara otomatis. Merupakan kode dari produk/konten yang dibeli oleh konsumen |
| Nama Produk | Data ini diisi oleh sistem secara otomatis. Merupakan nama produk/konten yang dibeli oleh konsumen |
| Jumlah Pembelian | Data ini merupakan jumlah konten yang dibeli oleh konsumen. Seorang konsumen dimungkinkan untuk membeli lebih dari satu lisensi konten (terutama jika konten tersebut berupa software) |
| Alamat Konsumen | Data ini secara default diisi oleh sistem berdasarkan pada data yang diperoleh saat konsumen melakukan |

| | |
|---|---|
| | registrasi, namun dapat dirubah sendiri oleh konsumen |
| Lokasi Konsumen | Data ini merupakan data yang dapat diperoleh jika konsumen menggunakan perangkat yang mengandung GPS (jika tidak, data ini bernilai kosong) |

Selanjutnya proses pembelian akan berlangsung seperti pada umumnya, seperti pemberian jumlah tagihan serta metode pembayaran.

Ketika seorang konsumen melakukan pembelian konten, secara otomatis akan dilakukan pembentukan *digital signature*. Setiap konten akan memperoleh dua buah *digital signature* dengan proses sebagai berikut:

| |
|---|
| *Digital Signature 1* = Bit Data Konten<br><br>*Digital Signature 2* = Kode Produk + ID konsumen + Alamat Konsumen + Lokasi Konsumen (jika ada) |

Setiap data *digital signature* yang ada akan disimpan dalam satu database khusus. Hal ini berguna jika suatu waktu produsen butuh untuk melakukan pelacakan. Pembentukan dua buah *digital signature* dimaksudkan untuk dua tujuan yang berbeda. *Digital signature* yang pertama, yang dibentuk dari bit data konten bertujuan untuk melakukan pemeriksaan apakah konten tersebut telah mengalami perubahan isi atau tidak. Sementara *digital signature* yang kedua dibentuk dengan tujuan untuk melacak siapa penyebar konten bajakan yang beredar (karena *digital signature* kedua tidak dipengaruhi oleh nilai data, maka *digital signature* ini tidak akan dapat berubah dengan mudah).

Proses pembentukan *digital signature* ini dilakukan dengan menggunakan *public key* milik produsen yang diambil oleh sistem secara otomatis dari data produsen.


*Gambar 5*
*Tampilan Fitur Pembelian Konten*

4. Rancangan Fitur Pemeriksaan Pembajakan

Pada fitur ini, seorang produsen dapat melakukan pemeriksaan jika dia mencurigai apakah terjadi pembajakan terhadap konten mereka ataukah mungkin telah terjadi perubahan terhadap isi konten. Syarat utama yang diperlukan untuk melakukan proses ini adalah produsen tersebut haruslah memiliki konten yang diduga telah dibajak atau dimodifikasi tersebut (konten bajakan yang beredar). Berikut data yang diperlukan untuk melakukan proses pemeriksaan tersebut:

| | |
|---|---|
| Upload Produk | Data ini berupa produk terbajak yang diupload ke dalam sistem oleh produsen |
| ID Produsen | Data ini merupakan ID produsen yang harus dimasukkan untuk memastikan bahwa produsen tersebut adalah produsen yang valid terhadap produk ini |
| ID Produk | Data ini merupakan ID dari produk yang harus dimasukkan oleh produsen |
| Private Key | Data ini merupakan *private key* yang dimiliki oleh produsen. Kesalahan pada *private key* akan menyebabkan proses pelacakan menjadi gagal |

Pasca input data diatas, sistem akan melakukan proses pemeriksaan terhadap konten tersebut. Pemeriksaan pertama adalah melakukan pemeriksaan terhadap *digital signature 1* dari konten. Sistem akan melakukan proses pembentukan ulang *digital signature 1* berdasarkan bit data konten saat itu. Jika ternyata terjadi perbedaan *digital signature*, maka dapat dipastikan konten tersebut telah mengalami perubahan isi.

Pemeriksaan yang kedua adalah dengan melakukan pemeriksaan terhadap *digital signature 2* dan melakukan perbandingannya dengan data dalam database. Dengan pemeriksaan ini, pelaku pembajakan dan perubahan isi konten dapat diketahui.


*Gambar 6*
*Tampilan Fitur Pemeriksaan Pembajakan*

5. Rancangan Fitur Penyalinan Konten

Pada fitur ini, seorang konsumen yang memiliki konten dengan *copy protection*, dapat melakukan proses penyalinan konten melalui sistem ini. Seperti yang diketahui, jika sebuah konten telah diberikan *copy protection*, maka konten tersebut tidak akan dapat disalin secara manual oleh konsumen selaku pembeli konten. Namun, demi menanggulangi kebutuhan pemindahan konten ataupun *backup* terhadap konten, seorang produsen dapat memberikan kebijakan dengan mengizinkan penyalinan konten melalui sistem dengan jumlah tertentu (berdasarkan data yang dimasukkan oleh produsen saat pendaftaran konten).

Jika seorang konsumen akan melakukan penyalinan konten, berikut data yang harus diberikan:

| | |
|---|---|
| Upload Produk | Data ini merupakan upload produk yang akan disalin yang dilakukan oleh konsumen. Fitur ini juga berperan untuk memeriksa apakah produk yang diunggah tersebut benar-benar produk yang dibeli oleh konsumen atau bukan |
| Jumlah Copy | Data ini merupakan jumlah salinan konten yang dibutuhkan oleh konsumen |

Jika jumlah copy yang dimasukkan oleh konsumen masih memenuhi ambang batas yang ditentukan oleh produsen, maka proses penyalinan konten akan dilakukan dengan prosedur sebagai berikut:

1. Sistem akan melakukan pembentukan ulang *digital signature* terhadap masing-masing penyalinan. Perbedaan terdapat pada *digital signature 2* dimana kode produk akan ditambah dengan kode *copy*, misalkan:
   Kode produk awal : ASD123FB
   Kode produk baru : ASD123FB-1 (copy ke-satu)
   Selanjutnya *digital signature* akan dibentuk persis seperti langkah saat pembelian konten.
2. Pasca pemberian *digital signature*, konsumen dapat mengunduh salinan konten tersebut melalui sistem.


*Gambar 7*
*Tampilan Fitur Penyalinan Konten*

6. Rancangan Digital Signature

*Digital signature* yang digunakan dalam sistem ini merupakan *digital signature* yang dibuat dengan menggunakan algoritma El Gamal dan SHA-256. Proses pembentukan *digital signature* dilakukan dengan proses sebagai berikut:

1. Penghitungan Nilai Hash
   Proses pertama yang dilakukan adalah penghitungan nilai hash dari data yang ada. Untuk proses pembentukan *digital signature 1* data yang diambil adalah bit data dari konten. Sementara untuk pembentukan *digital signature 2* data yang diambil adalah kode produk, ID konsumen, alamat konsumen serta lokasi lonsumen (jika ada).
2. Enkripsi Dengan El Gamal
   Proses selanjutnya adalah melakukan enkripsi terhadap kedua buah nilai hash yang diperoleh. Enkripsi tersebut dilakukan dengan menggunakan algoritma El Gamal dengan menggunakan *public key* yang dimiliki oleh produsen.
3. Penyisipan Digital Signature
   Selanjutnya dilakukan proses penyisipan terhadap *digital signature* ke dalam konten. Pada hasil akhir akan diperoleh dua buah *digital signature* yang tersisipkan di dalam konten tersebut.

## VII. Uji Coba Sistem

Pasca proses implementasi, penulis melakukan proses uji coba dengan beberapa jenis konten seperti PDF dan DOCX. Berikut hasil uji coba yang penulis lakukan:

### A. Uji Coba Konten PDF

Uji coba ini dilakukan penulis untuk sebuah konten bertipe PDF yang tentu saja tidak bersifat *editable*. Dalam tahap awal uji coba terlebih dahulu penulis melakukan pembuatan dua buah akun, yaitu satu akun produsen dan satu akun konsumen.

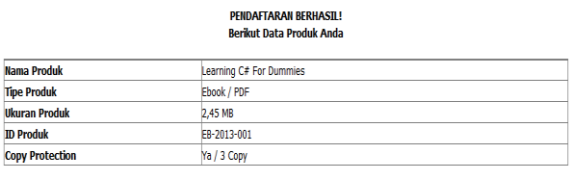
Akun produsen yang penulis gunakan memiliki *public key* dan *private key* sebagai berikut:

| |
|---|
| Public Key : 374495BD0000F47231483FAA<br>Private Key : 00000302374495BD |

Perangkat yang penulis gunakan adalah *tablet* yang memiliki fitur GPS sehingga memungkinkan untuk melakukan pelacakan lokasi. Berikut proses uji coba yang penulis lakukan:

1. Pendaftaran Produk

   Pada tahap awal penulis melakukan pendaftaran produk dengan pemberian *copy protection* dan jumlah *copy* maksimal 3 buah. Pasca pendaftaran ini, penulis memperoleh ID produk dari produk yang penulis daftarkan.




*Gambar 8*
*Tampilan Hasil Pendaftaran Konten*

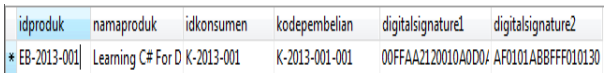
2. Pembelian Produk

   Selanjutnya penulis melakukan uji coba pembelian produk dengan menggunakan perangkat berfitur GPS dengan tampilan sebagai berikut:


*Gambar 9*
*Tampilan Proses Pembelian Produk*

Pasca pembelian produk, penulis akan mendapatkan sebuah link unduh khusus untuk mengunduh konten tersebut. Konten yang penulis unduh ini adalah konten yang telah memiliki *digital signature*.

Dengan mengamati database sistem, penulis memperoleh data mengenai *digital signature* dari file tersebut sebagai berikut:



| idproduk | namaproduk | idkonsumen | kodepembelian | digitalsignature1 | digitalsignature2 |
|---|---|---|---|---|---|
| * EB-2013-001 | Learning C# For D | K-2013-001 | K-2013-001-001 | 00FFAA2120010A0D0A | AF0101ABBFFF010130 |

*Gambar 10*
*Tampilan Database Sistem*

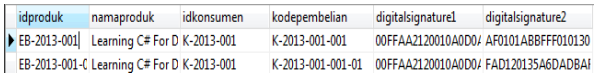
Dapat dilihat pada gambar diatas, terdapat perbedaan dari *digital signature 1* dan *digital signature 2*.

3. Penyalinan Konten

   Karena konten yang diujicobakan adalah konten yang diberi *copy protection*, maka jika seorang konsumen ingin melakukan penyalinan konten, konsumen tersebut harus melakukannya melalui sistem. Pada uji coba kali ini penulis mencoba melakukan penyalinan konten dengan hasil sebagai berikut:


*Gambar 11*
*Tampilan Proses Penyalinan Konten*

Pasca proses tersebut, penulis mendapatkan sebuah link unduh untuk konten baru yang telah tersalin. Jika diamati dalam database sistem, penulis mendapatkan sebuah data baru yang berisi *digital signature* baru terhadap konten yang telah disalin sebagai berikut:



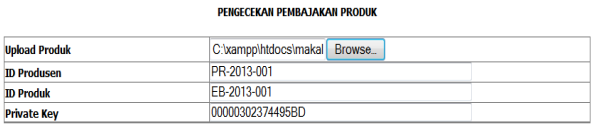
| idproduk | namaproduk | idkonsumen | kodepembelian | digitalsignature1 | digitalsignature2 |
|---|---|---|---|---|---|
| EB-2013-001 | Learning C# For D | K-2013-001 | K-2013-001-001 | 00FFAA2120010A0D0A | AF0101ABBFFF010130 |
| EB-2013-001-0 | Learning C# For D | K-2013-001 | K-2013-001-001-01 | 00FFAA2120010A0D0A | FAD120135A6DADBAF |

*Gambar 12*
*Tampilan Database Sistem*

Dengan mengamati gambar diatas, dapat dilihat terdapat perbedaan pada *digital signature 2* karena id produk sekarang telah bertambah dengan kode *copy*. Sementara *digital signature 1* tidak berubah karena konten tersebut masihlah konten yang sama.

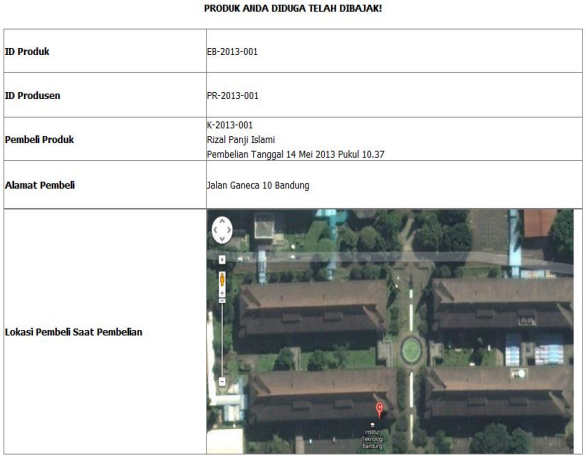
4. Pelacakan Pembajakan

   Uji coba terakhir yang penulis lakukan untuk konten ini adalah uji coba seandainya produsen menemukan sebuah konten yang diduga merupakan hasil pembajakan. Dalam uji coba ini penulis bertindak selaku produsen yang melakukan uji coba terhadap sebuah konten yang diduga telah dibajak dengan proses sebagai berikut:




*Gambar 13*
*Tampilan Pelacakan Pembajakan*

*Private key* yang digunakan untuk uji coba kali ini adalah *private key* yang diperoleh saat proses registrasi akun produsen. Pasca proses validasi, penulis memperoleh kesimpulan akhir sebagai berikut:




*Gambar 14*
*Tampilan Hasil Pelacakan Pembajakan*

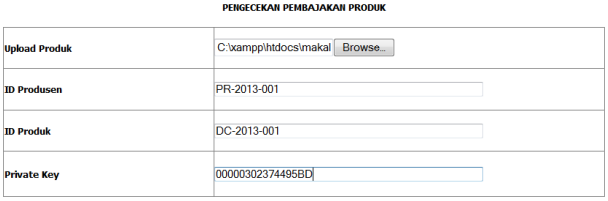
Dapat diamati dalam gambar diatas, produsen dapat mengetahui bahwa konten yang mereka jual diduga telah dibajak. Pembajakan diketahui dilakukan oleh konsumen dengan ID tercantum diatas. Selain itu, alamat konsumen dan juga lokasi pembelian produk yang dilakukan oleh konsumen dapat diketahui oleh produsen. Pasca proses ini, produsen dapat mengambil tindakan lebih lanjut, seperti permintaan untuk pemblokiran akun konsumen tersebut dan mungkin hingga pelaporan ke pihak yang berwenang.

## B. Uji Coba Konten DOCX

Uji coba selanjutnya yang penulis lakukan adalah uji coba menggunakan konten DOCX yang bersifat *editable* (dapat diedit). Tujuan dari uji coba kali ini adalah untuk memeriksa apakah sistem dapat mengenali konten yang telah mengalami perubahan isi atau tidak.

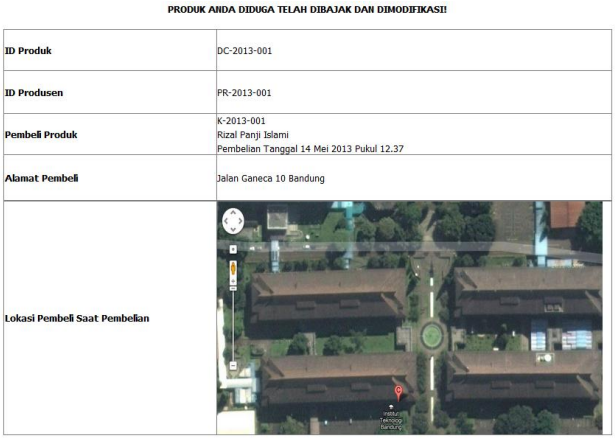
Proses awal uji coba dilakukan sama persis dengan uji coba pada bagian sebelumnya, namun perbedaannya uji coba dilakukan dengan menggunakan sebuah file DOCX yang *editable*.

Konten tersebut terlebih dahulu didaftarkan dan diuji cobakan untuk dibeli oleh konsumen. Selanjutnya, uji coba akan difokuskan pada kasus dimana produsen menemukan sebuah konten yang mirip dengan konten yang diproduksi oleh produsen tersebut. Produsen ingin memeriksa apakah konten tersebut merupakan konten mereka dan apakah konten tersebut telah mengalami modifikasi isi ataukah tidak. Berikut adalah hasil uji coba yang dilakukan:




*Gambar 15*
*Tampilan Pelacakan Modifikasi Konten*

Dapat dilihat pada gambar diatas, uji coba kali ini menggunakan konten dengan ID Produk yang berbeda, ID ini telah diperoleh sebelumnya saat melakukan proses pendaftaran produk. Saat dilakukan proses validasi, penulis memperoleh hasil sebagai berikut:




*Gambar 16*
*Tampilan Hasil Pelacakan Validasi Perubahan Konten*

Dapat dilihat dalam gambar diatas bahwa penulis berhasil mendapati bahwa konten tersebut telah mengalami pembajakan dan modifikasi konten. Selanjutnya produsen dapat mengambil tindakan lebih lanjut seperti pengajuan untuk memblokir akun pembeli ataupun melaporkannya ke pihak yang berwenang.

## VIII. SIMPULAN DAN SARAN

Berdasarkan hasil rancangan, implementasi dan uji coba yang telah dilakukan dalam protokol ini, dapat disimpulkan bahwa protokol digital signature untuk mekanisme pelacakan pembajakan hak cipta digital telah berhasil dilakukan. Terbukti melalui uji coba ini, dengan sebuah desain protokol yang khusus dan dengan mengandalkan konsep *digital signature*, proses pembajakan dan modifkasi terhadap konten digital dapat teramati dan terdeteksi. Pelaku pembajakanpun dapat diketahui dengan mudah karena proses penjualan dan pembelian produk dilakukan melalui protokol yang sama.

Proses perancangan protokol dan uji coba lebih lanjut masih perlu untuk dilakukan, terutama terkait dengan uji

coba terhadap konten berukuran besar serta desain lain yang berkaitan dengan segala peluang pembajakan yang mungkin dilakukan.

## REFERENSI


[1] Sadikin, Rifki. 2012. Kriptografi Untuk Keamanan Jaringan. Yogyakarta : Penerbit Andi

[2] Schildt, Herbert. 2007. *Java – The Complete Reference*. New York : Mc Graw Hill

[3] Welling, Luke. 2003. *PHP and MySQL Web Development*. New York : Sams Publishing


## PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 14 Mei 2013

Rizal Panji Islami
13510066