Seminar Nasional Royal (SENAR) 2018 ISSN 2622-9986 (cetak)
STMIK Royal – AMIK Royal, hlm. 1 – 6 ISSN 2622-6510 (online)
Kisaran, Asahan, Sumut - 3 September 2018

IMPLENTASI ALGORITMA CRC 32 DALAM MENGIDENTIFIKASI KEASLIAN FILE

Sri Wahyuni[1], Akhyar Lubis [2], Supina Batubara[3], Iqbal Kamil Siregar[4]
[1,2]Teknik Komputer, Universitas Pembangunan Panca Budi
[3]Sistem Komputer, Universitas Pembangunan Panca Budi
[4]Sistem Komputer, STMIK Royal Kisaran
email: [1]sriwahyuni@dosen.pancabudi.ac.id, [2]akhyarlbs.ac.id, [3]supinabatubara@dosen.pancabudi.ac.id, [4]iqbalkamilsiregar@royal.ac.id

Abstrak: *Proses pengiriman dan penyimpanan data dapat beresiko terjadi perubahan dan kehilangan data. Dalam menjaga dan mendeteksi kerusakan data, dapat dibuat sebuah aplikasi yang dapat mendeteksi kerusakan serta integritas data, digunakan suatu cara untuk menghitung suatu nilai terhadap data yang diberikan dan nilai tersebut dikirim bersama-sama data untuk dicek oleh penerima apakah data yang diterima sama dengan aslinya. Banyak fungsi algoritma hash yang dapat kita gunakan untuk proses mencari keaslian dan keamanan file. Salah satu algoritma yang dapat digunakan yaitu CRC (Cyclic Redundancy Check). CRC memiliki beberapa varian bergantung pada bilangan polynomial yang digunakan dalam proses komputasinya. Pada penelitian ini menggunakan CRC 32. Nilai 32 sendri memiliki arti sebagai nilai dari Polynomial yang bernilai 32 bit, nilai tersebut akan digunakan dalam proses komputasinya. Secara umum prinsip kerja dari CRC 32 adalah menganggap suatu file yang akan diproses sebagai suatu string yang besar, dimana string tersebut terdiri dari bit – bit. Nilai bit tersebut kemudian digunakan sebagai nilai yang akan dibagi oleh bilangan poly dengan operasi XOR.*

Kata kunci: *Keamanan Data, Algoritma CRC 32, Bit, String*

PENDAHULUAN

Data bagi organisasi adalah hal yang sangat penting. Data adalah aset berharga yang harus dilindungi (A. P. U, Siahaan ; 2018). Pengiriman data harus terjaga keaslian dan keamanan dalam komunikasi data, perlu dihindari dari akses oleh pihak yang tidak berhak. Pada saat pengiriman atau penyimpanan data dapat beresiko terjadi perubahan yang tidak diinginkan terhadap data. Untuk menjaga keaslian dan keamanan data kita dapat mengunakan algoritma yang dikembangkan untuk mendeteksi keaslian ataupun kerusakan data dalam proses transmisi data maupun penyimpanan data. Kita juga dapat menggunakan proses authentication pada informasi yang kita dapat agar kita mengetahui keaslian dari informasi tersebut. Salah satu cara yang dapat digunakan dalam menjaga keasliaan dan keamanan data dapat dilakukan dengan Algoritma CRC 32.

Dapat dibuat sebuah aplikasi yang dapat mendeteksi kerusakan serta integritas data, agar data yang digunakan tetap terjaga keaslian digunakan suatu cara untuk menghitung suatu nilai terhadap data yang diberikan dan nilai tersebut dikirim bersama-sama data untuk dicek oleh penerima apakah data yang diterima sama dengan aslinya (tidak mengalami kerusakan selama perjalanan atau penyimpanan). Kerusakan data ini biasanya hanya terjadi pada satu atau dua bit saja, maka untuk menghitung nilai data tersebut tidak perlu digunakan suatu fungsi algoritma yang benar-benar aman (rumit). Banyak fungsi algoritma hash yang dapat kita gunakan untuk proses mencari keaslian dan keamanan file. Disini penulis mengangkat salah satunya fungsi algoritma yang biasa digunakan yaitu CRC (Cyclic Redundancy Check). CRC memiliki beberapa varian bergantung pada bilangan polynomial yang digunakan dalam proses komputasinya. Pada penelitian ini menggunakan CRC 32.

Nilai 32 sendri memiliki arti sebagai nilai dari Polynomial yang bernilai 32 bit, nilai tersebut akan digunakan dalam proses komputasinya. Secara umum prinsip kerja dari CRC 32 adalah menganggap suatu file yang akan diproses sebagai suatu string yang besar, dimana string tersebut terdiri dari bit – bit. Nilai bit tersebut kemudian digunakan sebagai nilai yang akan dibagi oleh bilangan poly dengan operasi XOR.

Tujuan dari penelitian ini adalah untuk membuat aplikasi yang dapat mengecek

ISSN 2622-9986 (cetak)
ISSN 2622-6510 (online)

integritas sebuah data yang ingin ditransmisikan atau disimpan dan untuk meminimalkan kemungkinan penerimaan data yang telah dimodifikasi oleh pihak ketiga.

METODOLOGI

Keamanan informasi adalah suatu keharusan yang harus diperhatikan terutama jika informasi itu bersifar rahasia. Ketika suatu data dikirim melalui jaringan internet, data akan mengalami beberapa proses, proses tersebut terbagi oleh 7 layer yang tidak saling bergantungan antara satu sama lain tetapi saling berkaitan atau sering disebut 7 Layer OSI (Open System Interconnection). Model referensi OSI terdiri dari 7 buah bagian (Layer), yang masing – masing layer mempunyai tugas sendiri – sendiri, yang dibagi menjadi dua bagian yaitu proses encapsulation dan proses decapsulation. karena begitu kompleks proses dari pengiriman data, membuat proses tersebut tidak aman dari pihak ketiga, atau mengalami kerusakan dalam proses pengirimannya. Permasalahan ini membuat sebuah aplikasi yang dapat memeriksa file yang dikirim, agar file yang dikirimkan tersebut terjaga integritasnya atau keasliannya. Untuk memulai membangun suatu program mengenai keaslian file, maka penulis terlebih dahulu merencanakan alur kerja dari aplikasi yang akan dibangun agar mempermudah pembuatan aplikasi kedepannya.

CRC (Cyclic Redundancy Check) adalah algoritma untuk memastikan integritas data dan mengecek kesalahan pada suatu data yang akan ditransmisikan atau disimpan. Data yang hendak ditransmisikan atau disimpan ke sebuah media penyimpanan rentan sekali mengalami kesalahan, seperti halnya noise yang terjadi selama proses transmisi atau memang ada kerusakan perangkat keras. Sebelum masuk kedalam perancangan ada beberapa hal yang harus kita ketahui sebagai dasar dari perancangan algoritma yaitu prinsip kerja pada algoritma CRC, Pada intinya dalam proses penghitungan CRC. Kita menganggap suatu file yang kita proses sebagai suatu string yang besar, yang terdiri dari bit-bit, dan kita operasikan sebagai suatu bilangan polynomial yang sangat besar. Untuk menghitung nilai CRC, kita membagi bilangan polynomial, sebagai representasi dari file, dengan suatu bilangan polynomial kecil yang sudah terdefinisi untuk jenis varian CRC tertentu. Operasi pencarian nilai CRC menggunakan XOR, sisa nilai dari hasil operasi XOR antara Register dengan Poly disebut dengan checksum. Ada beberapa jenis perhitungan CRC yaitu sebagai berikut :

1) Perhitungan CRC Secara Aljabar. Untuk melakukan penghitungan CRC terhadap suatu data, maka yang pertama kita perlukan adalah suatu bilangan polinom yang akan menjadi pembagi dari data yang akan kita olah (kita sebut sebagai ‘poly’). Data yang kita olah mungkin saja hanya beberapa bit saja, lebih kecil dari nilai poly yang kita gunakan. Hal ini akan menyebabkan kita tidak mengolah semua nilai poly yang telah ditentukan. Untuk mengatasi hal tersebut, dalam penghitungan dasar secara aljabar, kita menambah suatu string bit sepanjang W pada data yang akan kita olah, untuk menjamin keseluruhan data kita proses dengan benar.
Poly = 10011 (width W=4)
Bitstring + W zeros = 110101101 + 0000

Contoh pembagian yang dilakukan:

```
10011/1101011010000\110000101
      10011|||||||| -
      -----||||||||
       10011|||||||
       10011|||||||  -
       -----|||||||
        00001||||||
        00000||||||   -
        -----||||||
         00010|||||
         00000|||||    -
         -----|||||
          00101||||
          00000||||     -
          -----||||
           01010|||
           00000|||      -
           -----|||
            10100||
            10011||       -
            -----||
             01110|
             00000|        -
             -----|
              11100
              10011         -
              -----
               1111 -> sisa hasil bagi
```

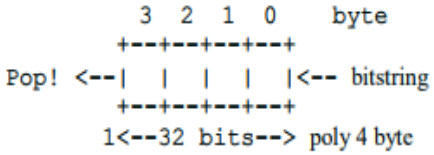
Gambar 1. Perhitungan CRC dengan Aljabar
Sumber : Indra Sakti Wijayanto (2014 : 3)

Sisa dari operasi XOR diatas merupakan nilai CRC yaitu 1111 yang merupakan hasil sisa bagi dari register dengan nilai poly. Adapun pada peroses pembagian diatas ada

ISSN 2622-9986 (cetak)
ISSN 2622-6510 (online)

aturan tertentu yaitu kita tidak perlu melakukan operasi XOR ketika bit tertinggi bernilai 0, tetapi kita hanya melakukan pergeseran (shift) sampai didapat bit tertinggi yang bernilai 1, adapun dalam pendekatan aljabar dibutuhkan waktu yang sangat lama dan tidak efficient. Hal ini dapat diperbaiki dengan menggunakan operasi berbasis byte, hal tersebut akan dibahas dalam pendekatan tabel CRC.

2) Pendekatan Tabel CRC. Dalam pendekatan tabel CRC Poly yang kita gunakan pun akan kita operasikan dalam bentuk byte, sehingga harus mempunyai panjang kelipatan 8 bit (byte), sebagai contoh dalam CRC32, kita akan menggunakan poly 32 bit (4 byte), akan tampak sebagai berikut :



Gambar 2. Pendekatan Model CRC 32
Sumber : Indra Sakti Wijayanto (2014 : 3)

Pada 4 ruang kosong diilustrasikan sebagai register yang akan kita gunakan untuk menampung hasil CRC sementara pada peroses pembagian tetap menggunakan operasi XOR, pada umumnya operasi diatas sama seperti proses operasi aljabar hanya saja dilakukan dengan pendekatan byte.

Sebagai contoh, kita akan memproses sebuah CRC 8 bit (poly hanya 1 byte) agar lebih mudah dipahami karena hanya terjadi sekali shift kita akan menggeser sebanyak 4 bit.

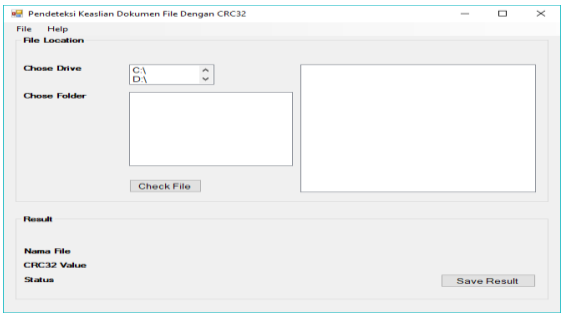
Isi awal register : 10110100
Setelah dilakukan pergeseran (nilai register) : 01001101
4 bit yang digeser (top bits) : 1011
Poly yang digunakan (W = 8) : 101011100

HASIL DAN PEMBAHASAN

Implementasi Program dapat dilihat langkah-langkah sebagai berikut :

1) Tampilan Halaman Utama Aplikasi Pemeriksa Keaslian File

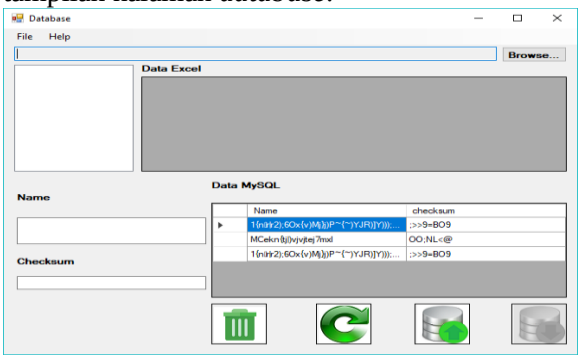
Halaman ini merupakan tampilan pertama kali muncul ketika program aplikasi dijalankan. Halaman utama dirancang untuk mencari File yang ingin di check keasliannya serta menginput data kedalam database



Gambar 3. Halaman UtamaAplikasi

2) Tampilan Halaman Database Aplikasi Pemeriksa Keaslian File.

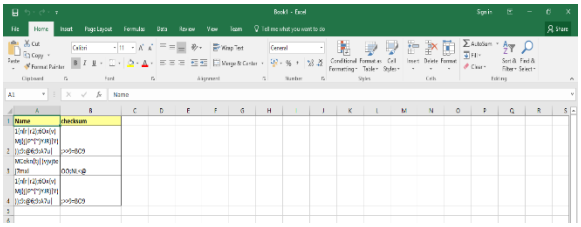
Halaman database, halaman database dirancang untuk proses import, export database serta untuk menghapus *record* data, berikut ini tampilan halaman *database*.



Gambar 4. Halaman Database Aplikasi

3) Tampilan Halaman Export Database Ke MS.Excel.

Pada Halaman ini lembar kerja dari MS.Excel berisi dari record (data) dari database File yang akan dikirim, adapun isi dari record diacak sehingga pengguna lain tidak dapat mengetahui nilai dari record tersebut.

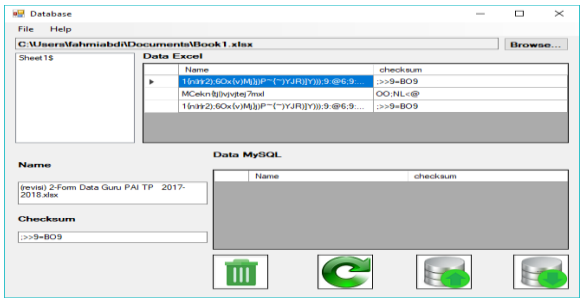


Gambar 5. Tampilan Halaman Export

4) Tampilan Halaman Import Database

Pada halaman Import Database memperlihatkan isi dari File yang akan di import menjadi database, adapun nilai yang dapat dilihat hanya nama dari File tersebut, hal itu sudah cukup untuk mengetahui apakan File tersebut adalah database yang dimaksud pengirim.

ISSN 2622-9986 (cetak)
ISSN 2622-6510 (online)



Gamabar 6. Halaman Import Database

Pembahasan harus mengeksplo-rasi signifikan sihasilpenelitian.Sebaik-nya berikan kutipan dari penelitian penelitian terdahulu yang dapat mendu-kung hasil dari penelitian anda.

Sumber Pustaka/Rujukan

Dokumen Digital

Menurut Hariyanto dalam jurnal berjudul Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, isi File Dokumen, dan File Dokumen Menggunakan Algoritma Advanced Encryption Standart Dokumen digital merupakan setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan dan/atau didengar melalui komputer atau sistem elektronik, tetapi tidak terbatas pada tulisan, suara atau gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti dan dapat dipahami oleh orang banyak (2015 : 2).

Checksum

Checksum adalah teknologi untuk menandai sebuah file, dimana setiap file yang sama harus memiliki checksum yang sama, dan bila nilai checksumnya berbeda meskipun satu bit saja, maka file tersebut merupakan file yang berbeda walaupun memiliki nama file yang sama.

Menurut Prihardhanto dalam Jurnal Aplikasi Otomatisasi Maintenance Perangkat Lunak dengan Fungsi Heuristic Intregrity Checkers dan Logika Fuzzy C-Mean (2013 : 3) Checksum atau Hash sum adalah suatu data dengan ukuran tetap yang dihitung dari suatu data dengan ukuran tetap yang dihitung dari suatu blok data digital dengan tujuan untuk mendeteksi kesalahan yang mungkin terjadi saat proses transmisi atau penyimpanan.

Checksum digunakan untuk verifikasi suatu data yang disimpan atau yang dikirim dan diterima. Setiap kali terjadi proses pengiriman data, checksum akan mengenali file tersebut untuk melihat apakah data yang diterima sudah sesuai dengan data yang dikirimkan. Fungsi inilah yang menjadikan checksum sangat efektif untuk melakukan pengecekan terhadap proses transfer suatu data.

Checksum akan membaca ulang, menghitung dan membandingkan file yang diterima dengan file yang ditransfer. Bila ada perbedaan nilai, maka checksum akan menganggap bahwa telah terjadi kesalahan, distorsi atau korupsi selama penyimpanan atau pengiriman.

Fungsi checksum akan selalu menghasilkan checksum dengan panjang yang tetap dan cukup identik satu sama lain. Dengan kata lain, bila pesan yang dimasukan berbeda, maka checksum-nya juga akan berbeda.

CRC 32 (Cyclic Redundancy Check 32)

CRC (Cyclic Redundancy Check) adalah algoritma untuk memastikan integritas data dan mengecek kesalahan pada suatu data yang akan ditransmisikan atau disimpan. Data yang hendak ditransmisikan atau disimpan ke sebuah media penyimpanan rentan sekali mengalami kesalahan, seperti halnya noise yang terjadi selama proses transmisi atau memang ada kerusakan perangkat keras.

Menurut H. P. Tarigan dalam Jurnal Penggunaan Metode Heuristik dan Cyclic Redudancy Check 32 (CRC 32) untuk Mendeteksi Kerusakan File, Cyclic Redundancy Check merupakan fungsi hash yang dikembangkan untuk memastikan integritas data dan mendeteksi kerusakan pada suatu file digital yang ditransmisikan atau disimpan.

CRC bekerja secara sederhana, yakni dengan menggunakan perhitungan matematika terhadap sebuah bilangan yang disebut sebagai Checksum, yang dibuat berdasarkan total bit yang hendak ditransmisikan atau yang hendak disimpan.

CRC didesain sedemikian rupa untuk memastikan integritas data terhadap degradasi yang bersifat acak dikarenakan noise atau sumber lainnya (kerusakan media dan lain-lain). CRC tidak menjamin integritas data dari ancaman modifikasi terhadap perlakukan yang mencurigakan oleh para hacker, karena memang para penyerang dapat menghitung ulang. checksum dan mengganti nilai checksum yang lama dengan yang baru.

ISSN 2622-9986 (cetak)
ISSN 2622-6510 (online)

CRC 32 merupakan salah satu algoritma Cyclic Redundancy Check yang menghasilkan checksum sebesar 32 bit. Prinsip utama yang digunakan CRC 32 adalah dengan melakukan pembagian polinomial dengan mengabaikan bit-bit carry sampai menghasilkan nilai.

CRC menggunakan prinsip modulo bilangan. Data dianggap sebagai sebuah bilangan, dan untuk menghitung checksum, sama dengan menambahkan digit untuk data dengan digit untuk checksum (berisi 0) kemudian dibagi dengan pembilang tertentu, dan sisa pembagiannya menjadi checksum untuk data tersebut. Tergantung pemilihan bilangan pembagi, CRC dapat mendeteksi single-bit error, double bit error, error berjumlah ganjil, burst error dengan panjang maksimum r. Bilangan pembagi tersebut disebut sebagai generator (polinomial).

Dalam penghitungan CRC, operasi pengurangan dan penjumlahan dilakukan dengan melakukan operasi XOR pada bit-bit, jika operasi tersebut ekivalen dengan operasi pengurangan pada aljabar biasa. Perhitungan CRC juga mengabaikan bit carry setelah bit tersebut melewati suatu operasi.

Pada CRC 32, generator pembagi data sering disebut generator polinomial karena nilai pembagi ini dapat direpresentasikan dalam bentuk polinomial peubah banyak, tergantung pada jenis atau nilai pembagi yang digunakan

Sumber pustaka/rujukan sedapat mungkin merupakan pustaka-pustaka terbitan 5 tahun terakhir. Pengutipan daftar pustaka sebaiknya berasal dari jurnal dalam jangka waktu lima tahun terakhir.

Berdasarkan analisa yang penulis lakukan terhadap proses kerja CRC 32 dalam melakukan pendeteksian kerusakan terhadap sebuah file, terdapat kelebihan dan kelemahan CRC 32. Kelebihan dari metode ini, yaitu :

1) CRC 32 merupakan metode yang sangat akurat dalam mendeteksi kerusakan terhadap sebuah file. Dengan menggunakan nilai checksum sebuah file, dimana nilai checksum merupakan identitas file tersebut, metode ini dapat mendeteksi perubahan-perubahan yang terjadi pada file tersebut.
2) CRC 32 merupakan metode yang sangat cocok untuk digunakan dalam mendeteksi kerusakan sebuah file yang disebabkan oleh serangan virus. Karena sebagian besar virus menyerang file dengan cara mengubah nilai checksum file tersebut, untuk mengubah atribut file atau mengubah struktur file yang terinfeksi, CRC 32 dapat mendeteksi pada bagian mana perubahan yang terjadi pada file berdasarkan hasil perbandingan fungsi hash dari nilai cheksum file tersebut dengan nilai checksum yang diperoleh dari registry sistem.
3) Karena kemampuannya dalam mendeteksi perubahan yang terjadi pada sebuah file berdasarkan nilai checksum file tersebut,CRC 32 dapat dijadikan sebagai tameng untuk mencegah sebuah virus menyerang sistem komputer. Karena sebagian besar virus menggunakan sebuah file autorun untuk menginfeksi sistem komputer, CRC 32 dapat digunakan untuk mendeteksi dan menangkal setiap file yang tidak terdaftar dalam registry sistem sehingga tidak memperoleh akses untuk memasuki system.

Adapun kekurangan dari CRC 32 dalam melakukan pendeteksian kerusakan terhadap sebuah file, sebagai berikut :

1) CRC 32 tidak dapat mendeteksi kerusakan dua atau lebih file sekaligus. Hal ini dapat mengakibatkan waktu pendeteksian yang sangat lama bila file yang ada dalam satu folder atau drive memiliki jumlah yang sangat banyak.
2) CRC 32 tidak dapat mendeteksi dengan baik file yang memiliki nilai fungsi hash diatas 32 bit. Pada pendeteksian kerusakan sebuah file yang memiliki nilai fungsi hash 128, 192 atau 256 bit hasil yang diperoleh tidak akan seakurat file yang memiliki nilai fungsu hash 32 bit kebawah.

SIMPULAN

Bedasarkan hasil pengujian aplikasi pemeriksa keaslian file dapat digunakan dalam mendeteksi keaslian file dari modifikasi pihak tertentu. Apalikasi ini dapat meminimalisir pengguna (user) terinfeksi malware dari file yang di terima karena telah dimodifikasi oleh pihak yang tidak bertanggung jawab.

UCAPAN TERIMA KASIH

Penelitian ini merupakan hasil dari penelitian mandiri, terimakasih kepada LPPM (Lembaga Penelitian dan Pengabdian

ISSN 2622-9986 (cetak)
ISSN 2622-6510 (online)

Masyarakat) Universitas Pembangunan Panca Budi yang telah mendanai penelitian mandiri.

DAFTAR PUSTAKA

A. P. U. Siahaan and S. Ariza, (2018). *Combination of levenshtein distance and rabin-karp to improve the accuracy of document equivalence level*. International Journal of Engineering & Technology, 2018 Vol.7 (2.27) pp. 17-21.

K. Saputra S, and A. Buono (2016). *Fuzzy-based Spectral Alignment for Correcting DNA Sequence from Next Generation Sequencer*. Journal of TELKOMNIKA, Vol.14, No.2, pp. 707~714.

Hariyanto (2015). *Implementasi Kriptografi Pengamanan Data Pada Pesan Teks isi File Dokumen, dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard*. pp.2.

Prihardhanto (2013). *Aplikasi Otomatisasi Maintenance Perangkat Lunak dengan Fungsi Heuristic Intregrity Checkers dan Logika Fuzzy C-Mean*, pp. 3.

Wahyuni, S. (2018). *Implementation of Data Mining to Analyze Drug Cases Using C4.5 Decision Tree*. Journal of Physics Conference Series. 970(1):012030.

Batubara, S. (2018). *Sistem Pakar Diagnosa Penyakit Dalam Dengan Solusi Pengobatan Tradisional*. SNITIK.

H. P. Tarigan (2016). *Penggunaan Metode Heuristik dan Cyclic Redudancy Check 32 (CRC 32) untuk Mendeteksi Kerusakan File*"