p-ISSN:2527-5321
e-ISSN:2527-5941

PENGGUNAAN EVENT VIEWER PADA WINDOWS DALAM MENEMUKAN MASALAH

Nunu Kustian[1], Dedin Fathudin[2],, Erlin Windia Ambarsari[3]

[1,3]Universitas Indraprasta PGRI
Jl. Raya Tengah No. 80 Kelurahan Gedong Pasar Rebo Jakarta Timur
[2] Universitas Pamulang
Jl. Surya Kencana No.1 , Pamulang, Kota Tangerang Selatan, Banten
[1]kustiannunu@gmail.com, [2]dosen00398@unpam.ac.id , [3]erlinunindra@gmail.com

ABSTRAK

Perangkat komputer menjadi kebutuhan masyarakat, untuk menyelesaikan pekerjaannya secara sistem yang terintegrasi. Masalah yang sering terjadi adalah pengguna komputer tidak mengetahui kerentanan sistem, diantaranya adalah aktivitas komputer yang tidak wajar; dalam hal ini, program yang tidak seharusnya dijalankan atau ada di komputer. Beberapa tahapan dapat digunakan untuk menganalisis aktivitas tersebut. Oleh karena itu, pada penelitian ini menggunakan Windows Event Viewer untuk Pengguna Sistem Operasi Windows sebagai pemecahan masalahnya. Event Viewer adalah modul snap-in dari Windows; utilitas yang digunakan untuk memeriksa kesalahan di kedua sistem dan aplikasi Windows. Event Viewer di Windows adalah salah satu alat yang digunakan untuk meninjau sistem individual dan administrator untuk memecahkan masalah melalui diagnostik log aktivitas abnormal yang sudah masuk dalam Event Viewer. Metode yang digunakan pada penelitian ini adalah forensik, yang dimana tujuannya adalah untuk menemukan kesalahan sistem berdasarkan skenario yang dibuat pada penelitian ini sebagai ilustrasi implementasi Event Viewer. Hasil yang didapatkan dari penelitian ini adalah Event Viewer dapat mendeteksi siapa saja yang berhasil masuk berdasarkan tanggal dan waktu sehingga perlu membatasi hak akses pada komputer yang digunakan.
Kata Kunci: Diagnosis, Event Viewer, Windows

ABSTRACT

Computer technology has become a societal requirement for completing tasks in an integrated. The difficulty is that many computer users are unaware of system vulnerabilities, such as anomaly computer activity or applications not operating on the machine. It may analyze the action in several phases. As a result, to solve the problem, the study employs Windows Event Viewer for Windows Operating System Users. Event Viewer is a Windows snap-in module that checks for faults in both the system and Windows apps. In Windows, Event Viewer is one of the tools administrators use to analyze personal computers and troubleshoot through diagnostics of aberrant activity logs previously documented in Event Viewer. The approach utilized in this study is forensics, to locate system problems using scenarios created to demonstrate the Event Viewer's implementation. According to the findings of this study, event Viewer can detect anybody who successfully entered based on the date and time required to limit access privileges on the computer used.
Key Word: *Diagnose, Event Viewer, Windows*

PENDAHULUAN

Sebelum adanya sistem operasi, manusia hanya menggunakan komputer dengan sinyal analog dan digital. Namun, seiring perkembangan ilmu teknologi muncul berbagai versi sistem operasi seperti Windows versi 10 Home, Pro, Student, MAC, dan Linux Ubuntu. Sistem operasi secara umum bertugas menjalankan dan mengelola program lain. Sistem operasi sebagai pengelola seluruh sumber daya yang terdapat pada setiap komputer dan menyediakan sekumpulan layanan atau *system call* kepada pengguna sehingga memudahkan dan memberi manfaat pada sumber daya sistem yang berfungsi sebagai media interaksi antara manusia dengan mesin yang tersusun dari metode dan komponen kerja.(Fitriyani, 2015).

Sistem operasi bersama dengan perangkat keras untuk membentuk sistem lengkap dalam menentukan tugas yang dioperasikan oleh komputer. Berdasarkan hasil statistik dari situs (https://netmarketshare.com, n.d.) pada tahun 2019 bulan Juli sampai tahun 2021 bulan Oktober penggunaan Windows mencapai 87,56% dibandingkan dengan penggunaan sistem operasi mac OS 9,54%, Linux 2,35%, Chrome OS 0,41%, unknown 0,13%, dan BSD 0,01%.

Berdasarkan statistik tersebut, Windows yang sering digunakan dalam melakukan tugas-tugas pekerjaan kantor maupun studi. Selain itu, Windows dapat menganalisis aktivitas yang terjadi secara langsung pada perangkat komputer pada saat sedang digunakan (O.O. et al., 2016). Permasalahan terjadi ketika pengguna Windows mengalami kendala saat *shutdown*, *startup*, dan komputer yang berjalan lambat. Oleh karena itu, terkadang sulit untuk dilacak sehingga penggunaan Event Viewer pada Windows perlu digunakan untuk meninjau dalam mendiagnosis peristiwa atau yang dikenal sebagai *log* terhadap perilaku yang mencurigakan pada sistem komputer. Event Viewer dapat berfungsi sebagai *desktop support* dan *help desk* untuk pencarian penyebab komputer yang mengalami *crash* secara *realtime*, mencatat *log*, dan merekam kejadian tersebut. Begitu juga dengan keamanan data, perlu di *monitoring* dan *auditing* pada personal komputer. Jika ada penggunaan hak akses yang dilakukan oleh pihak yang tidak berkepentingan, maka terjadi modifikasi data, pengrusakan data, maupun pencurian data pribadi.

Event Viewer memungkinkan pengguna untuk masuk dan membaca *file* sistem ketika Windows berjalan dan salah satu alat forensik digital untuk mengumpulkan data yang terkait pada sistem dan aplikasi yang digunakan oleh pengguna, kemudian dikumpulkan sebagai hasil penelusuran terhadap peristiwa-peristiwa yang terjadi dan menjadi bukti kesalahan maupun kejahatan dalam perangkat komputer (Raharjo, 2013). Beberapa teori pendukung sebagai penelitian yang relevan terkait sistem keamanan dan *log* yang direkam melalui alat analisis komputer, yaitu penelitian yang dilakukan (Do et al., 2014) dalam menganalisis Windows 7/8 dan Virtual Mesin Server 2008R2 dengan masing-masing Control Processing Unit i5 dan i7. Peristiwa yang diinvestigasi terdiri dari *key events*; *AntiMalware Update Events* pada Windows; *User Plug-n-Play Events*; *Networking Events*; Microsoft Office *Events*; dan *Group Policy Auditing Events* yang terdapat berbagai macam ID *Event* dari setiap peristiwa yang diteliti dengan berbagai informasi yang berbeda sebagai bukti proses forensik pada *logs* Windows dengan proses forensik peristiwa Windows (WinEFP) yang telah diusulkan lalu diterapkan ke hampir tiap penyelidikan yang melibatkan komputer pribadi Windows. Hasil dari penelitian ini menunjukkan bahwa forensik terhadap proses peristiwa dapat dipraktikkan, baik pada komputer personal maupun perusahaan-perusahaan besar setelah dikumpulkan, kemudian diidentifikasi data-data peristiwanya.

Penelitian yang dilakukan (Bhatele et al., 2019) menyelidiki serangan yang terjadi pada jaringan *internet* berbasis file *log* atau peristiwa yang menggunakan sistem operasi Windows disebabkan banyaknya pelaporan data-data penting yang hilang saat melakukan pekerjaan dalam suatu perusahaan, ancaman-ancaman yang terjadi menjadikan sebuah keuntungan bagi penyerang dari jaringan yang rentan dan dengan mudah mengakses sistem dengan mengubah atau menghapus data *log*. Untuk itu, diusulkan sebuah model struktural dari arsitektur sistem yang dapat membantu dalam memusatkan penyimpanan dan interpretasi *log* organisasi. Hasilnya, arsitektur yang diusulkan tersebut sangat efisien untuk menyederhanakan proses manajemen *log*, keterbatasan dari layanan *log event* di Windows dapat dengan mudah diatasi dalam solusi yang diusulkan dan dapat dengan mudah bahwa arsitektur tersebut diperluas di masa depan untuk perangkat lain.

Windows Event Viewer merupakan tempat penyimpanan semua peristiwa yang terjadi pada sistem operasi mulai dari sistem dibuka sampai ditutup. Permasalahan-permasalahan operasi seperti *crash* atau disebut *Blue Screen of Death* (Halsey, 2016). Oleh karena itu, pemeriksaan berbagai macam log pada sistem komputer yang digunakan dimana aplikasi dan sistem operasi yang bersangkutan dapat mencatat lebih dari satu log (Herbert & Vaughn, 2005). Log yang tampil di Event Viewer akan tampil otomatis secara terperinci berisi informasi peristiwa-peristiwa pada laptop atau PC.

Berdasarkan beberapa penelitian tersebut, terdapat beberapa kesamaan dimana menggunakan Event Viewer pada Windows untuk manajemen *log* komputer, tetapi penelitan ini melakukan pemeriksaan peristiwa-peristiwa yang terjadi seperti *log* aplikasi; *log* keamanan; *log* sistem; dari

p-ISSN:2527-5321
e-ISSN:2527-5941

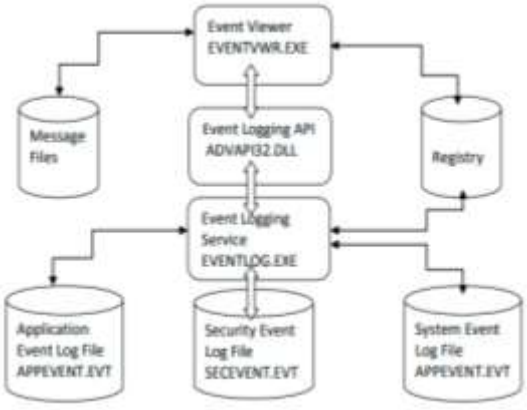
komputer personal dengan tujuan untuk mengidentifikasi permasalahan yang ditemui dalam *log event* terhadap perangkat komputer yang dimiliki dan memperbaiki permasalahan tersebut beserta solusinya. Maka penelitian ini menggunakan sebuah alat yang disediakan Windows yaitu Event Viewer dalam menemukan, mencatat, menyimpan peristiwa aktivitas yang terjadi pada komputer personal dengan sistem operasi Windows versi 10 Pro.

METODE PENELITIAN

Metode yang digunakan dalam penelitian ini dengan proses forensik *Event* Windows (Lucideus, 2018) dimana langkah-langkah penelitian ini dilakukan sebagai berikut:

1. Melakukan studi literatur tentang Event Viewer dan Windows.
2. Mengidentifikasi versi sistem operasi *Log event* bisa saja berbeda dari sistem operasi lainnya berdasarkan versi dan konfigurasinya.
3. Mengimplementasi Event Viewer dalam menganalisis peristiwa Windows dan mengetahui apa yang dicari di dalam daftar peristiwa.
4. Membuat keputusan dimana sistem yang sudah tercatat di dalam daftar peristiwa aman atau rentan terhadap bahaya selama jangka waktu tertentu.

Berikut cara kerja Event Viewer pada Windows:



Gambar 1. Interaksi Komponen *Logging Event* Windows dengan Aplikasi Win32 (EventVWR.EXE) (K.Sahoo et al., 2012)

Log dalam sistem di perangkat komputer merupakan semua tindakan seperti menghapus file, membuat file baru, menginstal perangkat lunak, dan mengetahui bagaimana pengguna masuk ke sistem, dimana semua tindakan ditulis ke dalam perangkat untuk tujuan audit sehingga dapat dilakukan kapan saja jika memerlukan beberapa pemecahan masalah seperti analisis forensik dan lain-lain. Tujuannya untuk mengetahui apa yang terjadi pada sistem. Detail informasi yang ditemukan di dalam *log* dalam setiap tindakan untuk setiap aktivitas akan ada satu *log* yang dihasilkan pada sistem, aktivitas *log* dapat terjadi pada komputer, *server*, *firewall*, dan lain sebagainya. *Log* adalah tindakan tunggal yang terjadi pada sistem, sedangkan peristiwa atau biasa dikenal dengan *event* merupakan perubahan perilaku sistem sehingga lebih dari satu *log* akan menjadi peringatan *event*.

Setiap *event* dapat dicatat di dalam catatan *log event* yang kemudian ditulis ke dalam *file log event* yang berasal dari *log event* itu sendiri. Sistem Windows mempunyai *log* Windows utama yaitu (Anson, 2019):

1. *Application*:
   Log aplikasi yang mencatat kesalahan yang terjadi di dalam aplikasi, kejadian informasi, dan peringatan dari aplikasi perangkat lunak.
2. *Security*:
   Berisi aktivitas *logon* dan *logoff*, dan aktivitas lain yang berhubungan dengan keamanan Windows.
3. *System*:
   Log sistem yang mencatat peristiwa dari segmen sistem operasi itu sendiri.

Pada penelitian ini menggunakan spesifikasi *framework* desktop personal seperti pada tabel 1.

Tabel 1. Spesifikasi Komputer

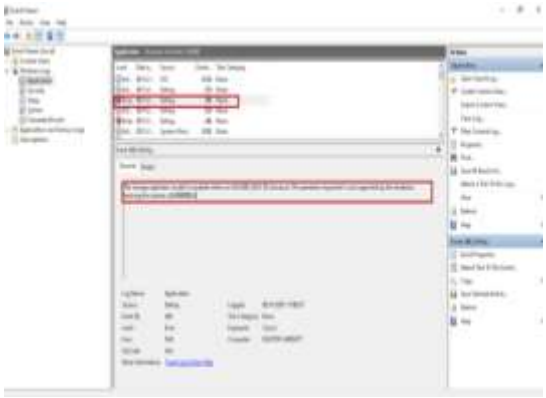
KOMPUTER	:	DEKSTOP
SISTEM OPERASI	:	WINDOWS 10 PRO VERSI 2004
CPU	:	INTEL® CORE I5
MEMORY		8GB
HDD	:	500GB
LOCAL DISK C	:	-
LOCAL DISK D		HOLMES_NUY

p-ISSN:2527-5321
e-ISSN:2527-5941

HASIL DAN PEMBAHASAN

1. Windows Log-*Application Log*

Pada prinsipnya, ketika menginstalasi program pada sistem operasi Windows telah membentuk *log*. *Log* tersebut disimpan di Event Viewer. Jadi, seseorang me-*restart* komputer dari jarak jauh; menghapus *log* audit; menghapus program; kesalahan instalasi. Akibatnya, dilacak oleh Event Viewer. Pada gambar 2, terdapat implementasi dari Event Viewer yang dianalisis melalui personal komputer:



Gambar 2. Windows Log: *Application Log*

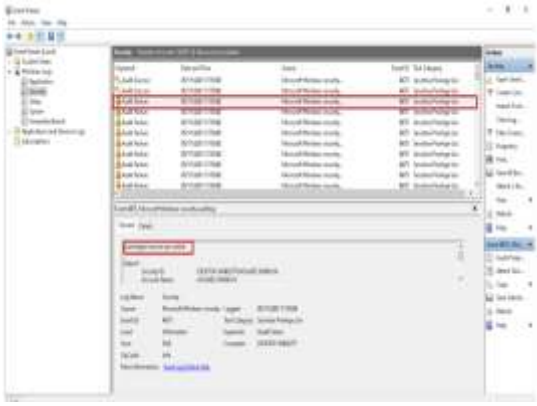
Gambar 2 menunjukkan notifikasi *Error* yang mencantumkan tanggal dan waktu pada *log* aplikasi, yakni 5 November 2021 pukul 17:00:27. Selanjutnya, penyimpanan tidak optimal dan tidak dapat menyelesaikan *retrim* pada *local disk* D (HOLMES_NUY). dikarenakan notifikasi event ID 264 yang mengartikan bahwa operasi yang diminta tidak didukung oleh perangkat keras yang mendukung *volume* (0x8900002A) (Corporation, n.d.-b)

Volume 0x8900002A adalah sebuah kode permasalahan yang menyatakan *drive* kemungkinan bermasalah sehingga tidak bisa melakukan pembaruan terhadap sistem operasi Windows karena *trim* pada *hard drive* tipe *platter* klasik tidak didukung saat *update* Windows versi 2004. Untuk mencari solusi pemecahan masalah dengan *event* ID yang sudah didapatkan, bisa dengan bantuan *platform* google.com yang menyediakan hasil penelusuran *event* ID 264.

Selanjutnya, penelitian ini dilakukan pencarian rujukan solusi melalui berbagai situs untuk memperbaiki event ID 264. Hasil yang didapatkan adalah menghapus instalasi perangkat lunak *antivirus*, mengkonfigurasi ulang tim jaringan, dan instalasi kembali perangkat lunak *antivirus* yang membutuhan jaringan koneksi *internet* (Corporation, n.d.-a). Namun, penanganan tersebut hanya batasan permanen.

2. Windows Log-*Security Log*

Ada dua jenis dari *security log*, yaitu *audit success* dan *audit failure*. Pada gambar 3 terdapat *audit success* yang terjadi karena sebuah akun berhasil *logoff* dan pada panel tercantum detail nama akun, misalkan HOLMES SHINICHI yang merupakan akun komputer lokal. Namun, terjadi juga *audit failure* dengan event ID 4673 yaitu *Sensitive Privilage Use* artinya Penggunaan Hak Istimewa yang dianggap oleh Microsoft, yang menunjukkan upaya dilakukannya operasi layanan sistem yang diistimewakan seperti *SeEnableDelegationPrivilege* yaitu pengguna dapat mengatur siapa saja pengguna atau komputer lain untuk melakukan delegasi pada komputer yang dimiliki, yaitu mengakses sumber daya dikomputer dengan pemberian wewenang yang sudah didelegasikan. Namun, pengguna atau objek yang diberikan hak istimewa ini harus memiliki akses tulis ke kontrol akses komputer tersebut. (Smith, Franklin, 2003).



Gambar 3. Windows Log: *Security Log*

Untuk memecahkan permasalahan yang terdapat pada *audit failure* dengan event ID 4673, berikut hasil yang didapatkan dari Microsoft Windows *Security Auditing* yang disajikan pada tabel 2.

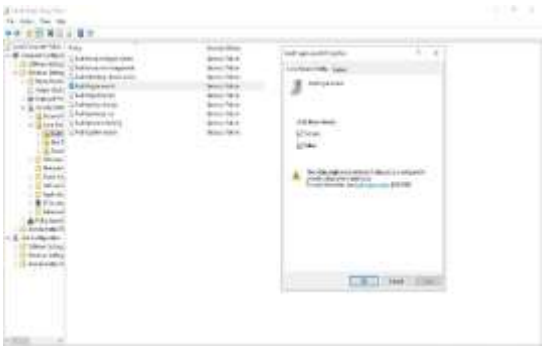
Tabel 2. Event ID 4673 Audit Failure

KATEGORI TUGAS	RESOLUSI
	1. BERTINDAK SEBAGAI BAGIAN DARI SISTEM OPERASI

p-ISSN:2527-5321
e-ISSN:2527-5941

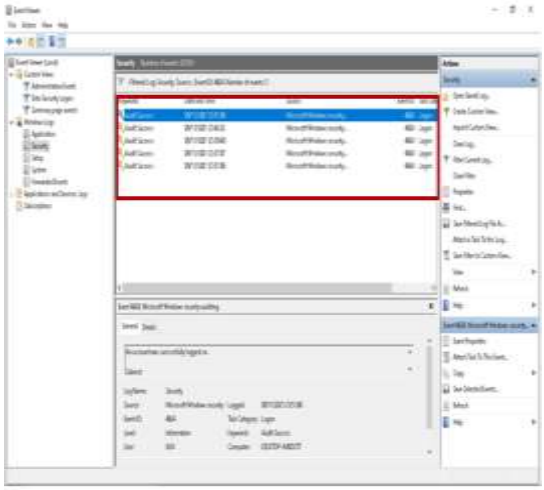
SENSITIVE PRIVILEGE USE	2. CADANGKAN FILE DAN DIREKTORI 3. BUAT OBJEK TOKEN 4. PROGRAM DEBUG 5. AKTIFKAN KOMPUTER DAN AKUN PENGGUNA AGAR DIPERCAYA UNTUK DIDELEGASIKAN 6. HASILKAN AUDIT KEAMANAN 7. MENIRU KLIEN SETELAH OTENTIKASI 8. MUAT DAN BONGKAR DRIVER PERANGKAT 9. KELOLA AUDIT DAN LOG KEAMANAN 10. UBAH NILAI LINGKUGNAN FIRMWARE 11. GANTI TOKEN TINGKAT PROSES 12. PULIHKAN FILE DAN DIREKTORI 13. AMBIL KEPEMILIKAN FILE ATAU OBJEK LAIN

Penelitian ini dibuatkan skenario dengan menyimulasikan pengguna yang berhasil masuk ke dalam personal komputer. Langkah-langkah dilakukan antara lain: Pertama, dibuat *Audit Logon events* melalui aplikasi *Local Group Policy Editor* yang merupakan sebuah alat dari Windows itu sendiri untuk mengatur panel yang ada di sistem operasi komputer; membatasi tindakan-tindakan yang tidak diinginkan yang menimbulkan ancaman keamanan komputer.
Kemudian, dilakukan *Audit Logon Event* dengan mengklarifikasi *audit success* dan *audit failure* yang terdapat pada gambar 4.



Gambar 4. *Local Group Policy Editor: Logon Audit Events*

Setelah itu, dengan Event Viewer lakukan *Filter Current Log* dengan event ID 4624 untuk mengetahui siapa saja yang telah masuk ke personal komputer.

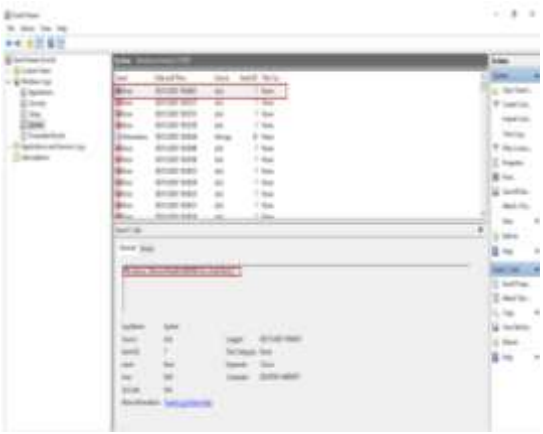


Gambar 5. Informasi *Logon Audit Events*

Pada gambar 5, terdapat informasi yang telah berhasil masuk ke komputer personal pada tanggal 09 November 2021 dengan beberapa kali waktu melakukan *logon* dengan berhasil. Namun, pemilik komputer tidak melakukan hal tersebut yang berarti ada pengguna yang tidak berhak mengontrol akses komputer tersebut secara diam-diam yang dapat mengakibatkan kerugian pada pemilik komputer.
Event Viewer tidak dapat mengetahui siapa yang melakukan penyusupan, tetapi dapat membantu pemilik komputer untuk menemukan hal-hal apa saja yang dilakukan oleh penyusup tersebut terhadap komputer yang dimilki. Oleh karena itu, dibutuhkan tindakan preventif untuk membatasi yang berhak melakukan akses ke komputer dan lebih waspada.

3. Windows Log-*System Log*
Suatu sistem harus sehat dalam pelayanan aplikasi yang penting. Sistem dapat mengalami kegagalan sehingga dibutuhkan pemantauan untuk mengganti *file* sistem; mengakibatkan *disk* yang rusak. Pada gambar 6 terdapat sistem *error* yang berasal dari *disk* dengan *event* ID 7 yang berarti bahwa Perangkat\Device\Harddisk\DR0 memiliki *badblock* atau kesalahan yang berasal dari *drive* pita yang kotor kemudian Windows berusaha untuk membaca *block* memori tersebut tetapi *block* data tersebut rusak atau hilang (Constantinos, n.d.).

p-ISSN:2527-5321
e-ISSN:2527-5941

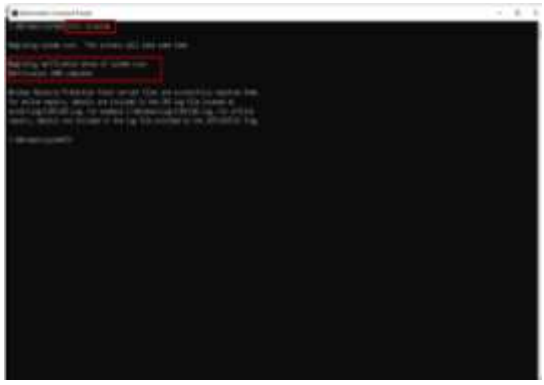


Gambar 6. Windows Log: *System Log*

Pencarian solusi seperti yang dilakukan sebelumnya, yaitu melalui situs untuk memperbaiki sistem *log event* ID 7 (Veritas & LLC, n.d.) dengan menjalankan CHKDSK utilitas yang dibangun didalam Windows untuk men-*scan* dan memperbaiki *harddisk* yang disebabkan oleh *badsector, software* yang *corrupt* dan metadata *corrupt*. CHKDSK di jalankan melalui *Command Prompt*.

Gambar 7. CHKDSK pada *Command Prompt*

Perintah pada gambar 7 memerlukan *reboot* pada sistem komputer yang akan di periksa lain waktu untuk dijadwalkan dalam memeriksa dan memperbaiki *harddisk* secara otomatis pada sistem *startup* selanjutnya.
Solusi kedua, adalah menjalankan *System File Checker* (SFC) yang dibangun juga oleh Windows sebagai utilitas yang menyediakan pengguna dalam me-*restore* sistem *file* yang *corrupt*.



Gambar 8. SFC pada *Command Prompt*

Proses pada gambar 8 memerlukan beberapa waktu sampai verifikasi 100% *completed*, kemudian dilakukan *restart* komputer dan setelah kembali *logon*, maka dilakukan pemeriksaan pada Event Viewer bahwa *error* yang terjadi pada *log* sistem sudah tidak ada.

Hasil dari penelitian ini Event Viewer dapat mengidentifikasi sesuai dengan skenario yang sudah disimulasikan dan dapat melakukan penanganan dalam *Security Log* dengan cara membatasi hak akses pada komputer yang digunakan.

SIMPULAN DAN SARAN

Event Viewer hanya menyajikan seputar pesan-pesan yang terjadi seperti kesalahan, peringatan, dan informasi pada aplikasi, keamanan, dan sistem pada Windows yang digunakan sehingga dapat disimpan pesan-pesan tersebut untuk mencari permasalahan yang terjadi pada komputer baik dari perangkat keras dan perangkat lunak yang di instalasi namun permasalahan terhadap pesan-pesan tersebut pencarian solusinya dengan bantuan *platform* google dengan rujukan-rujukan yang didapatkan karena sebagai pengguna Windows yang awam, tidak pernah tahu *log event* ID dari Windows tersebut, tetapi selama komputer yang dimiliki tidak memiliki kendala apapun, maka pengguna dapat terus menggunakan komputer untuk menjalankan aktivitas di dalam sistem operasi Windows komputer.
Disarankan perlunya pengkajian beberapa skenario yang melibatkan Event Viewer karena setiap perbaikan pada sistem tergantung *log event* yang dihasilkan pada Event Viewer.

DAFTAR PUSTAKA

Anson, S. (2019). Applied Incident Response. In *Applied Incident Response*. https://doi.org/10.1002/9781119560302

Bhatele, K. R., Shrivastava, H., & Kumari, N. (2019). *The Role of Artificial Intelligence in Cyber Security*. *April*, 170–192. https://doi.org/10.4018/978-1-5225-8241-0.ch009

Constantinos. (n.d.). *Fix: Event 7 Disk has a bad block at \Device\Harddisk#\DR#*. https://www.wintips.org/fix-event-7-disk-has-a-bad-block-at-device-harddisk/

Corporation, M. (n.d.-a). *Support Microsoft*. Support Microsoft. https://support.microsoft.com/

Corporation, M. (n.d.-b). *Windows Logs show Event ID 264 Warning*. Microsoft. https://social.technet.microsoft.com/Forums/ie/en-US/e3ef8088-56f3-4db1-9b0b-e440a1c8d792/windows-logs-show-event-id-264-warning?forum=w8itprohardware

Do, Q., Martini, B., Looi, J., Wang, Y., & Choo, K. K. (2014). Windows event forensic process. *IFIP Advances in Information and Communication Technology*, *433*, 87–100. https://doi.org/10.1007/978-3-662-44952-3_7

Fitriyani. (2015). Strategi Pemilihan Sistem Operasi Untuk Personal Computer. *JSM STMIK Mikroski*, *16*(1), 11. https://media.neliti.com/media/publications/280973-strategi-pemilihan-sistem-operasi-untuk-f8f02fbb.pdf

Halsey, M. (2016). Windows 10 Troubleshooting. In M. Halsey, Mike (Ed.), *Windows 10 Troubleshooting* (Series Edi). APRESS. https://doi.org/10.1007/978-1-4842-0925-7

Herbert, C., & Vaughn, L. (2005). *QUT Digital Repository : http://eprints.qut.edu.au/ 3800*. *11*, 1–8.

https://netmarketshare.com. (n.d.). *Operating System Market Share*.

K.Sahoo, P., K. Chottray, R., & Pattnaiak, S. (2012). Research Issues on Windows Event Log. *International Journal of Computer Applications*, *41*(19), 40–48. https://doi.org/10.5120/5650-8030

Lucideus. (2018). *Introduction to Event Log Analysis Part 1 — Windows Forensics Manual 2018*. Medium.Com. https://medium.com/@lucideus/introduction-to-event-log-analysis-part-1-windows-forensics-manual-2018-b936a1a35d8a

O.O., O., Ogunbanwo, A., Lateef, U., & G.O., O. (2016). Microsoft Windows Operating System. *The Cosit Text On Mathematics, Computer & Biology*, *October*, 138–146.

Raharjo, B. (2013). Sekilas Mengenai Forensik Digital. *Jurnal Sosioteknologi*, *12*(29), 384–387. https://doi.org/10.5614/sostek.itbj.2013.12.29.3

Smith, Franklin, R. (2003). Windows Security Log Event ID 4673. In *Windows Security Log Events*. https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4673

Veritas, & LLC, T. (n.d.). *What does Event ID 5/7/9/11/15 mean while troubleshooting tape device related issues with Backup Exec*. https://www.veritas.com/support/en_US/article.100028072