MEMBANGUN DAN MENGUJI WEB BROWSER DAN SERVER PADA ONION WEB SERVER (DEEPWEB)

Februrian[1], Joko Triyono.[2], Prita Haryani [3]

[1]Jurusan Teknik Informatika, Institut Sains & Teknologi AKPRIND Yogyakarta
Jl Kalisahak No. 28 Komplek Balapan Tromol Pos 45, Yogyakarta 55222 Telp : (0274) 563029
Email: februrian.co.id@gmail.com, jack@akprind.ac.id, pritaharyani@akprind.ac.id

Abstract

Website is one of the important aspects of internet life today. In the use of a website in general use data. Data is a very important resource for a person, so at the moment data is one of the vital objects in the internet. The system studied is one of the solutions of a server that has a high and secure privacy security system, so as to reduce the risk of data misuse. The system is named Tor, where the Tor system uses a different network than the website network in general. The type of data analysis method used in this research is quantitative analysis technique. Quantitative data analysis techniques are used to analyze observational data on compatibility and performance testing. In accordance with the characteristics of quantitative research, this research was conducted using a structured, formal, and specific design, and had a detailed operational design. In this study, there is also data that has been collected and analyzed which is quantitative in nature or can be quantified by calculations and measurements.

Keywords *: Tor, Website, Server*

Abstrak

Website merupakan salah satu aspek penting dalam kehidupan ber-internet saat ini. Dalam penggunaan sebuah *website* pada umumnya menggunakan data. Data merupakan sumber daya yang sangat penting bagi seseorang, sehingga pada saat ini data merupakan salah satu objek vital dalam ber-internet. Sistem yang diteliti merupakan salah satu solusi dari sebuah *server* yang memiliki sistem keamanan privasi yang tinggi dan aman, sehingga dapat mengurangi resiko penyalahgunaan data. Sistem tersebut bernama *Tor*, dimana sistem *Tor* tersebut menggunakan jaringan yang berbeda dari jaringan *website* pada umumnya. Jenis metode analisa data yang digunakan pada penelitian ini adalah teknik analisa kuantitatif. Teknik analisa data kuantitatif digunakan untuk menganalisa data hasil observasi pada pengujian *compatibility* dan *performance.* Sesuai dengan ciri – ciri dari penelitian kuantitatif penelitian ini dilakukan dengan menggunakan rancangan yang terstruktur, formal, dan spesifik, serta mempunyai rancangan operasional yang yang mendetail. Pada penelitian ini juga terdapat data yang telah dikumpulkan serta dianalisis yang bersifat kuantitatif atau dapat dikuantitatifkan dengan perhitungan serta pengukuran.

Kata Kunci : *Tor, Website, Server*

Pendahuluan

Sebuah *website* merupakan salah satu bentuk implementasi kemudahan dalam mendapatkan informasi secara langsung. Banyak media informasi yang telah tersedia, baik pada *local server* pada suatu insitusi tertentu, maupun secara global yang dikonsumsi khalayak banyak. Dengan *website* apapun informasi yang diinginkan akan tersedia baik secara gratis maupunn secara eksklusif (*premium content*).

Dengan kebutuhan akan data dan informasi tersebut seringkali banyak orang biasanya menyimpan data – data pribadi mereka pada *website* tersebut untuk keperluan pribadi maupun sebuah transaksi pada saat mereka menggunakan *website* tersebut, sehingga banyak sekali data personal yang disalahgunakan oleh pihak yang tidak bertanggung jawab. Segi keamanan *website* juga menjadi salah satu faktor penyebab kebocoran data. Namun hal yang lebih penting dari itu adalah pengguna itu sendiri yang menggunakan layanan tersebut.

Sebuah *website* juga seringkali menyimpan *log* dari pengunjung. IP Publik, data *login*, data personal serta seringkali dijumpai sebuah *website* ingin mendapatkan akses keperangkat keras baik kamera, mikrofon, lokasi dan lainnya yang sangat berbahaya bagi pengguna itu sendiri tanpa disadarinya. Kesalahan tersebut bisa berakibat sangat fatal baik dari integritas seperti contoh kasus yang paling fatal adalah penyadapan dan pemakaian informasi palsu seseorang sehingga merugikan seseorang.

Tinjauan Pustaka

Penelitian ini diadaptasi dari beberapa pustaka yang berupa jurnal maupun jenis karya tulis ilmiah lainnya yang telah ada sebelumnya dan relevan yang dijadikan acuan dalam penulisan penelitian ini, adapun penelian yang digunakan yaitu jurnal yang ditulis oleh Kautsarina (2017), menyimpulkan dalam jurnalnya, riset etnografi diranah maya tidak hanya dapat dilakukan pada obyek *surface web*, namun juga menarik untuk dapat dilakukan pada ranah *Dark Web*. Beberapa peneliti sebelumnya menunjukkan bagaimana metode etnografi dapat dilakukan pada area *Dark Web*, dan etika apa yang harus diperhatikan oleh peneliti. Ada yang menggunakan pendekatan teknis statistik dan ada juga yang melibatkan metode kualitatif.

Dari hasil penyelidikan oleh Aked (2011) pada Konferensi Prosiding mengungkapkan bahwa tampak bahwa situs media populer benar dalam menyatakan bahwa ada sejumlah besar konten ilegal yang mudah tersedia di *Darknets*. Popularitas pornografi anak sangat mengganggu, dan mengingat sifat alami *Darknets*, tampaknya penghapusan konten dan penuntutan terhadap mereka yang menawarkan konten tersebut akan sangat sulit. Perlu dicatat bahwa *Darknets* sendiri tidak menawarkan konten untuk diunduh oleh orang lain, juga pembuat aplikasi berbagi *file peer-to-peer,* keputusan itu tergantung pada individu yang berpartisipasi dalam jaringan. *Darknets* tidak harus dilihat sebagai sumber konten, melainkan saluran yang digunakannya untuk bepergian (komunikasi data). *Darknets* mudah dihubungkan, dan karena mereka menjadi lebih populer karena hambatan untuk menyusut, mereka yang menginginkan anonimitas akan dilayani dengan baik dimasa depan.

Sun, et al., (2019) mereka mengungkapkan fokus pada berbagi data aman menggunakan *geometricuting* di *darknets* dan mengusulkan kerangka kerja yang aman SeDS (*Secure Data Sharing*) dalam topologi hierarkis berdasarkan pada skema penyisipan *bit-string bitprefix* dua tingkat. Publikasi atau permintaan item data selalu dapat melewati node keamanan yang sesuai, sehingga strategi keamanan dapat dilakukan. SeDS menyediakan komunikasi *end-to-end* yang efisien dan berbagi data. SeDS tidak terbatas pada *darknets*, ia juga dapat digunakan untuk jaringan nirkabel atau sistem berbagi data lainnya. Karena SeDS hanya kerangka kerja aman tanpa skenario keamanan khusus dan strategi keamanan, bagaimana menggunakan SeDS untuk menyelesaikan masalah keamanan tertentu dapat menjadi pekerjaannya dimasa depan.

Website merupakan suatu dokumen berupa kumpulan halaman *web* yang saling terhubung dan isinya terdiri dari berbagai informasi berbentuk teks, suara, gambar, video, dan lainnya, dimana semua data tersebut disimpan pada *server* hosting (maxmanroe.com, 2020).

Deepweb atau juga yang biasa dikenal dengan darknet, *darkweb*, *tor server*, *invisible web*, *undernet*, *hidden web, onion web server* dan lainnya merupakan bagian dari WWW (*World Wide Web*) yang merupakan sebuah istilah yang digunakan dalam menyebut sebuah web yang berada pada jaringan *tor* dimana *website* tersebut tidak bisa diakses melalui *browser* pada umumnya dan hanya bisa diakses melalui *tor browser*. Ukuran *Deep Web* berdasarkan ekstrapolasi yang dilakukan oleh Universitas California, Berkeley pada tahun 2001 (California University, 2001) memperkirakan bahwa *Deep Web* memiliki ukuran sekitar 7,5 petabita . Ukuran yang lebih akurat disebutkan dalam penelitian yang dilakukan oleh Francisco Javier López Pellicer (2012) mendeteksi sekitar 300.000 situs *Deep Web* yang ada diseluruh Web pada tahun 2004 dan menurut Shestakov, sekitar 14.000 situs *Deep Web* berada dibagian web Rusia pada tahun 2006 (Shestakov, 2009).

Tor Network merupakan sekelompok *server* yang dioperasikan secara sukarela yang memungkinkan orang untuk meningkatkan privasi dan keamanan mereka di Internet. Pengguna *Tor* menggunakan jaringan ini dengan menghubungkan melalui serangkaian terowongan *virtual* daripada membuat koneksi langsung, sehingga memungkinkan organisasi dan individu untuk berbagi informasi melalui jaringan publik tanpa mengorbankan privasi mereka. Sejalan dengan

itu, *Tor* adalah alat pengelakan sensor yang efektif, yang memungkinkan para penggunanya untuk mencapai tujuan atau konten yang diblokir (Tor Project, 2020).

Sistem Informasi adalah suatu sistem yang menyediakan informasi untuk manajemen pengambilan keputusan/kebijakan dan menjalankan operasional dari kombinasi orang-orang, teknologi informasi dan prosedur-prosedur yang terorganisasi. atau sistem informasi diartikan sebagai kombinasi dari teknologi informasi dan aktivitas orang yang menggunakan teknologi untuk mendukung operasi dan manajemen. Sedangkan dalam arti luas, sistem informasi diartikan sebagia sistem informasi yang sering digunakan menurut kepada interaksi antara orang, proses, algoritmik, data dan teknologi (Anggraeni, 2017).

Tor Browser merupakan sebuah perangkat lunak *web browser* dari *Tor* Project yang menyembunyikan identitas *user* ketika sedang *online*. Hal ini dapat dilakukan dalam beberapa cara yang berbeda. Pertama, menggunakan enkripsi untuk mengacak data yang sedang dikomunikasikan dalam jaringan. Yang kedua, rute data antara *server* diatur secara acak dalam jaringan *Tor* untuk menyembunyikan identitas *online*, termasuk data terkait dengan alamat IP pribadi (Tor Project, 2020).

VPS (*Virtual Private Server*) merupakan sebuah teknologi dalam virtualisasi *server*. Sebuah *server* "fisik" dibagi menjadi beberapa *server virtual* sehingga setiap VPS terlihat bekerja seperti sebuah *server* mandiri, yang sebenarnya setiap VPS memiliki *Full Root Access*, *Operating System*, dan pengaturan sendiri dalam *user*, *script*, *Central Processing Unit (CPU)*, *Random Access Memory (RAM)* yang berdiri sendiri (Ricky Eka P, 2020).

SSH *(Secure Shell)* merupakan sebuah *Cryptography Network Protocol* dalam komunikasi data yang aman. Dengan *login interface* berbasis CLI, dimana sebuah perintah dieksekusi dari jarak jauh dan layanan jaringan lainnya antara komputer baik secara lokal maupun secara global. Aplikasi yang paling terkenal dari protokol ini adalah untuk akses ke akun *shell* pada sistem operasi mirip *Unix*, tetapi juga dapat digunakan dengan cara yang sama untuk akun pada Windows (Sudarmo, 2018).

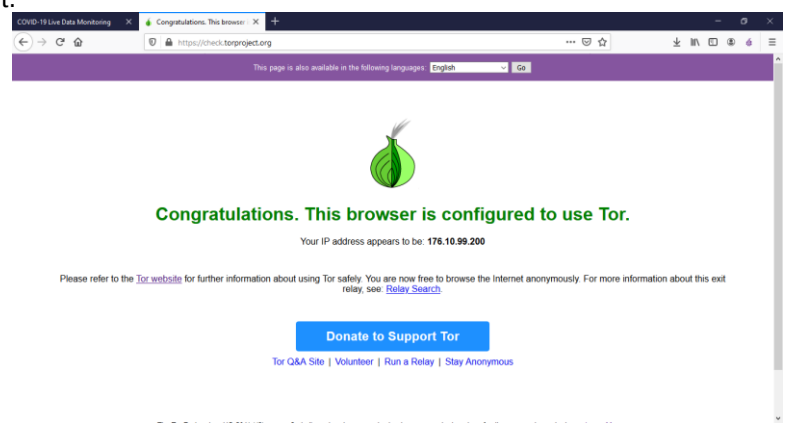
Pembahasan

Pengujian Pada *Server*

Konfigurasi Pengujian *Server*

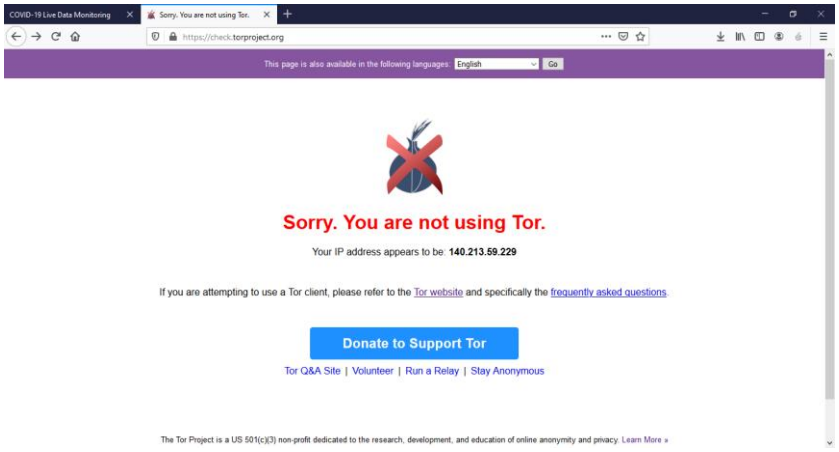
Pengujian *server* dilakukan dengan menggunakan sistem operasi Windows dimana sistem operasi ini merupakan sistem operasi yang paling awam digunakan. Dalam pengujian ini perangkat harus dapat terkoneksi kedalam jaringan tor dengan menggunakan sebuah *tool* yang diberikan oleh tor dalam mengkoneksikan perangkat komputer.

Dalam menguji sebuah perangkat komputer yang terkoneksi kedalam jaringan tor, dapat digunakan sebuah web yang telah disediakan oleh tor yang beralamatkan https://check.torproject.org/ , adapun contoh penggunaan dan hasil pengujian dalam dilihat dalam gambar berikut.



Gambar 1. Perangkat komputer yang terhubung ke tor

Gambar 1 adalah contoh dari perangkat komputer yang telah terhubung dengan jaringan tor.



Gambar 2. Perangkat komputer yang tidak terhubung tor

Gambar 2 menunjukan sebuah perangkat komputer yang tidak terkonesi pada jaringan tor.

Hasil Pengujian Koneksi

Pengujian koneksi tor pada *webserver* dapat dilakukan dengan tools pihak ketiga. Dalam pengujian ini gunakan tool yang ditulis menggunakan bahasa python yang bernama onioff. Onioff merupakan tool yang dikembangkan dalam memeriksa konektifitas dan ketersediaan sebuah website yang menggunakan jaringan tor

Hasil Pengujian Data Transfer

Pada pengujian data transfer digunakan tool yang bernama *nyx* yang telah disediakan secara resmi oleh tor dalam melihat data transfer yang digunakan oleh *browser* pada *server* tor. Dalam pengujian tersebut dapat diperoleh grafik daripada kecepatan download serta upload dari *browser* ke *server*. Dalam pengujian ini tidak sebagian *server* namun keseluruhan *server* dan tergantung pada kecepatan *server* dan koneksi internet.

CPU & Memory Usage (VPS)

Pada *Virtual Private Server* (VPS) dapat dilihat penggunaan CPU dan *memory* disaat administrator terkoneksi pada *server* melalui SSH. Penggunaan CPU dan *memory* pada VPS dapat menggunakan perintah *htstop*.

Pengujian Pada *Browser*

Hasil Pengujian *Compatibility*

Pengujian compatibility dilakukan dengan cara mengujicobakan aplikasi *tor browser* terhadap beberapa perangkat sistem operasi seperti android, IOS, Linux, Windows dan MacOS. Hasil pengujian tersebut didapat dengan melihat tingkat keberhasilan aplikasi tersebut dijalankan pada *screenshot* yang dilampirkan pada halaman lampiran. Hasil pengujian tersebut dirangkum kedalam beberapa tabel berikut.

Tabel 1. Hasil pengujian *Compatibility*

No	Sistem Operasi	Nama perangkat	Hasil Pengujian
1	Android 4.1.1	Google Galaxy Nexus	1
2	Android 4.4.2	Samsung Galaxy V	1
3	Android 10	Realme 3 Pro	1
4	IOS 11.3.1	IPhone 5	0
5	IOS 12.4.6	IPhone 5s	1
6	IOS 14.4	IPhone 6	1
7	Windows 10 Pro	ASUS X441UA	1
8	Windows XP Pro	ASUS X441UA	0
9	Kali linux Rolling 2020.1	ASUS X441UA	1
10	MacOS Catalina 10.15.3	ASUS X441UA	1

Berdasarkan data hasil pengujian yang telah diperoleh maka selanjutnya dapat dihitung persentase dari keberhasilan pengujian terhadap indikator yang diujikan.

Rumus :

$$Persentase\ kelayakan\ (\%) = \frac{Skor\ yang\ diperoleh}{Skor\ yang\ diharapkan} x\ 100\%$$

Maka dapat diperoleh hasil sebagai berikut :

$$Persentase\ kelayakan\ (\%) = \frac{8}{10} x\ 100\%$$

= 80 %

Dari persentase kelayakan dapat disimpulkan dari kategori kelayakan berdasarkan tabel kategori kelayakan, hasil dengan persentase 80% dimana dalam segi compatibility aplikasi ini termasuk kedalam klasifikasi Sangat Layak.

Hasil Pengujian Performance

Dalam pengujian dari segi performa pada aplikasi, digunakan beberapa aplikasi pihak ketiga dalam menguji kinerja aplikasi pada beberapa sistem operasi, dengan melihat aktifitas CPU dan memory pada perangkat yang digunakan. Dengan mengetahui hasil dari pengujian performance ini, dapat diketahui rata – rata penggunaan CPU dan memory pada perangkat dalam menjalankan *tor browser* sehingga dapat diketahui penggunaan aplikasi tersebut dapat dikatakan layak atau tidak.

Berdasarkan analisis dari penggunaan CPU aplikasi pihak ketiga, didapat hasil bahwa rata-rata penggunaan CPU oleh *tor browser* adalah sebagai berikut berdasarkan sistem operasi:

Pada sistem operasi android diujikan tor browser pada perangkat Realme 3 Proyang berspesifikasi Qualcomm SDM 710 Octa Core, RAM 4GB, ROM 64 GB. Pengujian aplikasi *tor browser* pada android dilakukan dengan aplikasi pihak ketiga yaitu Android Debug Brigde (ADB) dimana aplikasi ini merupakan aplikasi debugger yang memang resmi dari pihak android sendiri dalam melakukan debugging dalam melihat performa android maupun perintah lainnya. diperoleh penggunaan CPU dan memory aplikasi *tor browser* dibagi menjadi 2 (dua) proses yang dijabarkan pada Tabel 2.

Tabel 2. Penggunaan CPU dan Memory pada Android

No.	Nama proses aplikasi	Penggunaan CPU (%)	Penggunaan Memory (%)
1	libTor.so	4.6%	0.6%
2	org.torproject.+	1.0%	8.8%

Dari Tabel 2 dapat dihitung penggunaan total daripada CPU sebesar :

4.6 % + 1.0% = 5.6%

Dan total dari penggunaan Memory sebesar :

1.0% + 8.8% = 9.8%

Pengujian performance pada sistem operasi IOS pada perangkat IPhone dapat menggunakan aplikasi Lirum Device info yang bisa diunduh melalaui app store secara gratis. Pengujian *tor browser* dilakukan pada perangkat IPhone 5s dengan spesifikasi CPU Apple A7 S5L8960X Core 2 IOS 12.4.5 dengan RAM 1 GB dan ROM 16 GB. Perangkat yang menggunakan sistem operasi IOS sebelum menjalankan aplikasi *tor browser*, dengan penggunaan CPU awal sebanyak 47.25% dari total CPU pada perangkat dan 1.33% penggunaan memory dari 1GB RAM pada perangkat. penggunaan CPU dan memory setelah dijalankan *Tor browser* pada perangkat. Dari data tersebut didapatkan penggunaan CPU sebanyak 50.56% dan memory sebanyak 5.18% dari total 1GB memory pada perangkat. Maka dapat dihitung penggunaan CPU dan memory dari selisih persentase awal dan persentase akhir dari penggunaan CPU dan memory sebagai berikut.

Tabel 3. Penggunaan CPU dan Memory pada IOS

Keterangan	CPU (%)	Memory (%)
Penggunaan awal	47.25%	1.33%
Penggunaan akhir	50.76%	5.18%
Total penggunaan	3.51%	3.85%

Dari Tabel 3 dapat diketahui jumlah penggunaan CPU oleh *tor browser* sebanyak 3.51% dan penggunaan memory sebanyak 3.85%.

Pada pengujian Performance pada Windows digunakan aplikasi bawaan yang sudah ada pada sistem secara default, dengan menggunakan software task manager dapat dilihat

penggunaan rata – rata CPU dan memory. Pada pengujian ini digunakan sistem operasi Windows 10 Pro x64 4 GB RAM dan processor Intel ® Core ™ i3-6006U CPU @ 2.00 GHz 1.99 GHz. Proses yang dijalankan pada *tor browser* dimana terdapat 6 (enam) proses yang dijalankan pada perangkat, juga diperoleh penggunaan CPU sebanyak 0.9% dan penggunaan *memory* sebanyak 15.0% dari total keseluruhan yang tersedia pada perangkat.

Pada sistem operasi linux pada pengujian ini juga digunakan perangkat yang sama dengan sistem operasi Windows sebelumnya baik dari segi spesifikasi maupun jenis perangkat. Hasil yang didapatkan sudah tentu berbeda, dikarenakan paket penginstallan maupun performa dari sistem operasi itu sendiri. Pada pengujian ini digunakan sistem operasi linux yaitu Kali linux 2020.1 tepatnya.

Proses yang digunakan oleh *tor browser*, terdapat 4 (empat) sub-process dimana total dari ke-empat process tersebut menghasilkan total penggunaan CPU sebanyak 13% dan total penggunaan memory utama sebanyak 4% dijumlahkan dengan penggunaan RSS *memory* sebanyak 7% dengan total keseluruhan penggunaan memory sebanyak 11%.

Pengujian Performance atau kinerja pada sistem operasi MacOS digunakan sebuah aplikasi *software* bawaan dari MacOS itu sendiri yaitu *Activity Monitor*. Pada software tersebut didapatkan hasil pengujian sebagai berikut. Proses yang digunakan oleh *tor browser* yang dijabarkan kedalam tabel berikut :

Tabel 4. Penggunaan Memory pada MacOS

No.	Nama Proses	Penggunaan Memory (MB)
1	*Tor Browser*	139.7 MB
2	*Tor.real*	22.5 MB
	Total	162.2 MB

Total *memory* yang terdapat pada perangkat pengujian adalah 4.00 GB atau jika dikonversikan kedalam satuan MB berjumlah 4000 MB. Untuk menghitung jumlah persentase jumlah penggunaan *memory* yang digunakan oleh *tor browser* digunakan rumus persentase pada umumnya.

$$Persentase\ (\%) = \frac{f}{N}\ x\ 100\%$$

Keterangan :
f = Jumlah *Memory* yang digunakan
N = Total *memory* pada perangkat

Jika dimasukan kedalam rumus tersebut didapatkan hasil sebagai berikut :

$$Persentase\ (\%) = \frac{162.2}{4000}\ x\ 100\%$$
$$= 4.05\%$$

Maka penggunaan *memory* oleh *tor browser* adalah sebanyak 4.05% dari seluruh total penggunaan *memory* pada perangkat yang menggunakan sistem operasi MacOS.

Tabel 5. Hasil Pengujian *Performance*

No	Jenis Sistem Operasi	Parameter	Hasil pengujian (%)	Kesimpulan Hasil < 15%
1	Android	CPU	5.6 %	Sesuai
		Memory	9.8 %	Sesuai
2	IOS	CPU	3.51 %	Sesuai
		Memory	3.85 %	Sesuai
3	Windows	CPU	0.9 %	Sesuai
		Memory	15.0 %	Sesuai
4	Linux	CPU	13.0 %	Sesuai
		Memory	11.0 %	Sesuai
5	MacOS	CPU	6.9 %	Sesuai
		Memory	4.05 %	Sesuai

Hasil analisis dan pengujian dari sistem pendukung tor yaitu *tor browser* mendapatkan persentase kelayakan dari segi *compatibility* sebanyak 100% serta dapat diklasifikasikan sebagai

kategori sangat layak pada tingkat compatibility pada setiap perangkat yang diujikan.Hasil daripada analisis dan pengujian *tor browser* dari segi *Performance* juga mendapatkan hasil yang baik dan layak. Semua sistem operasi dari setiap perangkat menunjukan besarnya penggunaan CPU yang dibawah 15%. Dimana sistem akan berjalan dengan normal tanpa adanya kesalahan pada aplikasi maupun pada perangkat sehingga minimnya perlambatan pada *device*. Sedangkan penggunaan *memory* dibawah 15% menunjukan aplikasi ini hanya memakan sedikit penggunaan *memory* tanpa adanya (*crash / force close*).

Kesimpulan

Berdasarkan penelitian yang sudah dilakukan, dapat diambil beberapa kesimpulan berdasarkan rumusan masalah yang telah dijabarkan adalah sebagai berikut :

1. *Web application* yang digunakan pada jaringan tor memiliki kelebihan dan kekurangan, namun jauh lebih banyak kelebihan daripada *web application* yang dijalankan *server* biasa.
2. Banyak aspek – aspek yang dibutuhkan dalam membangun sebuah web application pada jaringan tor seperti halnya pada *server* pada umumnya seperti aspek keamanan, aspek privasi, aspek antarmuka dan lainnya,
3. Seperti web application pada umumnya aplikasi yang dibuat dengan jaringan *tor* dapat berjalan diberbagai sistem operasi dan perangkat serta memiliki kegunaan yang sama, namun perbedaan dasar pada umumnya terletak pada sistem keamanan privasi pada jaringan tor yang kuat. Dari *website* yang dibuat tidak mendapatkan kendala sedikitpun sehingga berjalan dengan baik dari *frontend* maupun *backend*.
4. *Tor browser* sebagai sarana dalam pengujian *tor server* hanya bisa digunakan pada sistem operasi tertentu dengan spesifikasi minimum : Windows 7 32 Bit pada sistem operasi Windows dan IOS IOS 11.3.1 pada IPhone. Pada spesifikasi sistem operasi diatasnya dan lainnya bisa digunakan secara normal dan maksimal.

Daftar Pustaka

Aked, S. (2011). AN INVESTIGATION INTO DARKNETS AND THE CONTENT AVAILABLE VIA ANONYMOUS PEER-TO-PEER FILE SHARING. *Australian Information Security Management Conference* (Pp. 10-18). Perth Western: Edith Cowan University.

Anggraeni, E. Y. (2017). *Pengantar Sistem Informasi.* Yogyakarta: ANDI.

California University. (2001). White Paper: The Deep Web: Surfacing Hidden Value. *Wall Street Journal Or The Economist*, Volume 7, Issue 1.

Dittipidsiber. (2020, 02 28). *Tribatanews Polri*. Retrieved From Tribatanews Polri: Http://Tribratanews.Polri.Go.Id/?P=466131

Francisco Javier López Pellicer, R. B. (2012). *Providing Semantic Links To The Invisible Geospatial Web.* Spain: Universidad Zaragoza.

Kautsarina. (2017). PERKEMBANGAN RISET ETNOGRAFI DI ERA SIBER : TINJAUAN METODE ETNOGRAFI PADA DARK WEB. *Jurnal Masyarakat Telematika Dan Informasi*, 145-158.

Maxmanroe.Com. (2020, February 11). *Teknologi*. Retrieved From Maxmanroe.Com: Https://Www.Maxmanroe.Com/Vid/Teknologi/Internet/Pengertian-Website.Html

Ricky Eka P, A. R. (2020). Virtual Private Server (VPS) Sebagaialternatif Pengganti Dedicated Server. *11th Seminar On Intelligent Technology And Its Applications, SITIA 2010*, 1-6.

Shestakov, D. (2009). On Building A Search Interface Discovery System. *VLDB Workshops* (Pp. 114-125). Lyon,France: VLDB .

Sudarmo, M. A. (2018). *Kumpulan Konfigurasi Debian Server.* Jakarta: Ampashi.

Sun, Y., Li, M., Su, S., Tian, Z., Shi, W., & Han, M. (2019). *Secure Data Sharing Framework Via Hierarchical Greedy Embeddingin Darknets.* China: National Natural Science Foundation Of China.

Tor Project. (2020, February 11). *Tor Project*. Retrieved From Tor: Https://2019.Www.Torproject.Org