CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 2, No. 1, Mei 2019, hlm. x-x

ANALISIS JARINGAN PADA APLIKASI PENGAMANAN AKSES INTERNET

Dedy Hariyadi[1], M. Roykhul Jinan[2], Nur Seto Bayuaji[3], Anas Sufi Hasan[4]

[1,2,3] *Fakultas Teknik dan Teknologi Informasi, Universitas Jenderal Achamd Yani Yogyakarta*
Email: [1]*milisdad@gmail.com,* [2]*roihul.unix@gmail.com,* [3]*bayuajins@gmail.com,* [4]*anassufi007@gmail.com*

(Naskah masuk: dd mmm yyyy, diterima untuk diterbitkan: dd mmm yyyy)

Abstrak

Pertumbuhan penggunaan internet di Indonesia selalu meningkat dari tahun ke tahun. Ancaman pada jalur internet perlu menjadi perhatian khusus. Salah satu serangan yang memungkinkan mengambil alih atau merekayasa informasi adalah *Man-in-the-Middle* (MITM). Untuk menghindari serangan MITM beberapa pengguna internet memasang aplikasi tambahan baik pada ponsel cerdas ataupun komputer. Aplikasi tambahan ini cara mendapatkannya ada yang bersifat gratis dan berbayar. Pada penelitian ini melakukan survei ke beberapa responden terkait implementasi aplikasi pengamanan akses internet di ponsel cerdas maupun komputer. Hasil survei juga diselaraskan dengan analisis trafik jaringan terkait metode-metode yang digunakan dalam aplikasi pengamanan akses internet. Aplikasi-aplikasi pengaman akses tersebut masing-masing memiliki metode untuk mengamankan dari serangan MITM.

Kata kunci: *Keamanan Informasi, Sensor, Virtual Private Network, DNS over HTTPS, SSH Tunneling, DNS over TLS, The Onion Router, DNSCrypt, Man-in-the-Middle*

NETWORK ANALYSIS ON INTERNET ACCESS SECURITY APPLICATIONS

Abstract

The growth of internet usage in Indonesia has always increased from year to year. Threats to the internet line need special attention. One attack that allows taking over or manipulating information is Man-in-the-Middle (MITM). To avoid MITM attacks some internet users install additional applications both on smartphones or computers. This additional application is a free and paid way to get it. In this study conducted a survey of several respondents related to the implementation of the application to secure internet access on smart phones and computers. The survey results are also harmonized with network traffic analysis related to the methods used in internet access security applications. The security access applications each have a method for securing MITM attacks.

Keywords: *Information Security, Censorship, Virtual Private Networks, DNS over HTTPS, SSH Tunneling, DNS over TLS, The Onion Router, DNSCrypt, Man-in-the-Middle*

1. PENDAHULUAN

Pertumbuhan jumlah pengguna internet di Indonesia dari tahun ke tahun selalu meningkat. Berdasarkan survei pada tahun 2017 pengguna internet sekitar 143,26 juta pengguna (Asosiasi Penyelenggara Jasa Internet Indonesia and Teknopreneur Indonesia, 2017) sedangkan pada tahun 2018 terjadi peningkatan menjadi sekitar 171,17 juta pengguna. Dari 171,17 juta pengguna perangkat yang digunakan untuk mengakses internet berupa ponsel cerdas sekitar 93,9% (Asosiasi Penyelenggara Jasa Internet, 2019). Menurut Masyarakat Telematika Indonesia (MASTEL) saluran penyebaran berita hoax di Indonesia pada tahun 2017 tiga besar melalui media internet, yaitu sosial media sebesar 92,4%, instant messenger sebesar 62,8% dan situs web sebesar 34.9% (Masyarakat Telematika Indonesia, 2017).

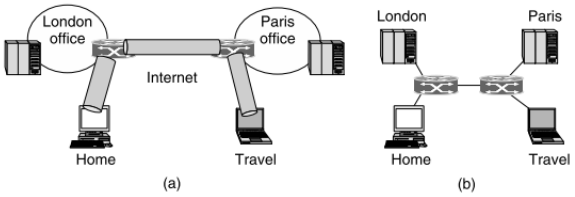
Berdasarkan siaran pers Kementerian Komunikasi dan Informatika Nomor 106/HM/KOMINFO/05/2019 bahwa akses instant

messenger dan sosial media dibatasi secara sementara dan terbatas untuk menanggulangi penyebaran berita hoax (Kementerian Komunikasi dan Informatika, 2019b). Walaupun pembatasan akses instant messenger dan sosial media secara terbatas memiliki dampak pengguna internet melakukan pemasangan perangkat lunak tambahan guna memperlancar komunikasi. Tiga hari kemudian pihak Kementerian Komunikasi dan Informatika melakukan normalisasi akses internet untuk instant messenger dan sosial media yang tertuang pada siaran pers nomor 107/HM/KOMINFO/05/2019 (Kementerian Komunikasi dan Informatika, 2019a). Pada siaran pers tersebut terdapat himbauan diantaranya tidak menggunakan perangkat lunak untuk terhubung ke jaringan melalui *Virtual Private Network* (VPN). Hal ini dikhawatirkan sistem pemantau, pengumpulan dan pembajakan akun atau data pribadi.

Virtual Private Network (VPN) memang diawalnya digunakan untuk melindungi privasi dalam mengakses internet, meningkatkan keamanan saat mengakses internet dan menghindari dari sistem sensor. Namun aplikasi VPN di Google Playstore[1] ditemukan melakukan aktivitas pelacakan, injeksi Javascript, pengalihan iklan, dan intersepsi TLS (Ikram et al., 2016).

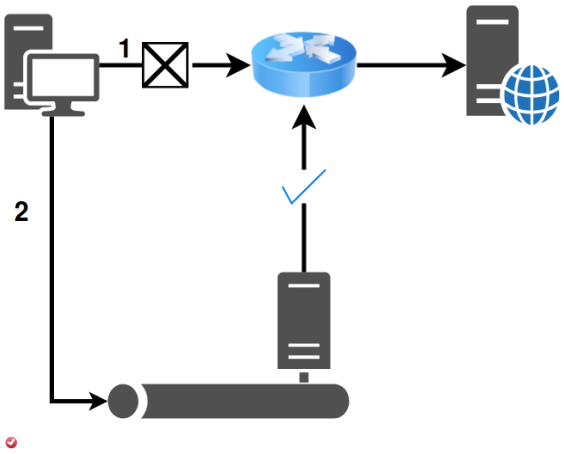
2. TINJAUAN PUSTAKA

Pada prinsipnya *Virtual Private Network* (VPN) merupakan teknologi jaringan komputer yang seolah-olah membuat jalur tersendiri pada infrastruktur publik dalam hal ini jaringan internet (Lewis, 2006) sehingga topologi *Virtual Private Networks* seperti terhubungnya dua perangkat router pada jaringan lokal. Gambar 1 menunjukan terhubungnya dua kantor di London dan Paris yang memanfaatkan teknologi VPN diatas jaringan internet (Tanenbaum dan Wetherall, 2011). Teknologi VPN dipilih salah satu alasanya adalah keamanan karena menggunakan metode tunneling dan enkripsi yang tidak mudah dibaca atau diintersep oleh pihak ketiga (Purbo, 2009). Alasan ini yang digunakan beberapa pengguna internet untuk mengalihkan sistem sensor yang diterapkan pada suatu organisasi atau institusi.



Gambar 1. (a) Koneksi VPN Dua Kantor (b) Topologi VPN Dipandang dari Internal

Metode *tunneling* yang melakukan pembungkusan *IP Datagrams* ke dalam *Frame Networks* yang selanjutnya dikirimkan ke *host* lainnya (Kent dan Atkinson, 1998) menjadi pilihan para pengguna internet mengalihkan sistem sensor. Implementasi sederhana dari metode *tunneling* adalah melakukan pembelokan akses melalui *SSH Server* yang memiliki akses tanpa pembatasan atau sensor. Sebagai contoh terlihat pada 2, saat komputer mengakses internet melalui jalur 1 tidak diperkenankan oleh router. Sehubungan komputer memiliki sebuah *server* pada jalur 2 yang memiliki protokol SSH dan dapat mengakses internet maka komputer tersebut dapat mengakses internet dengan melakukan tunneling ke *server* tersebut (Hariyadi, Subhan dan Vanca, 2018).



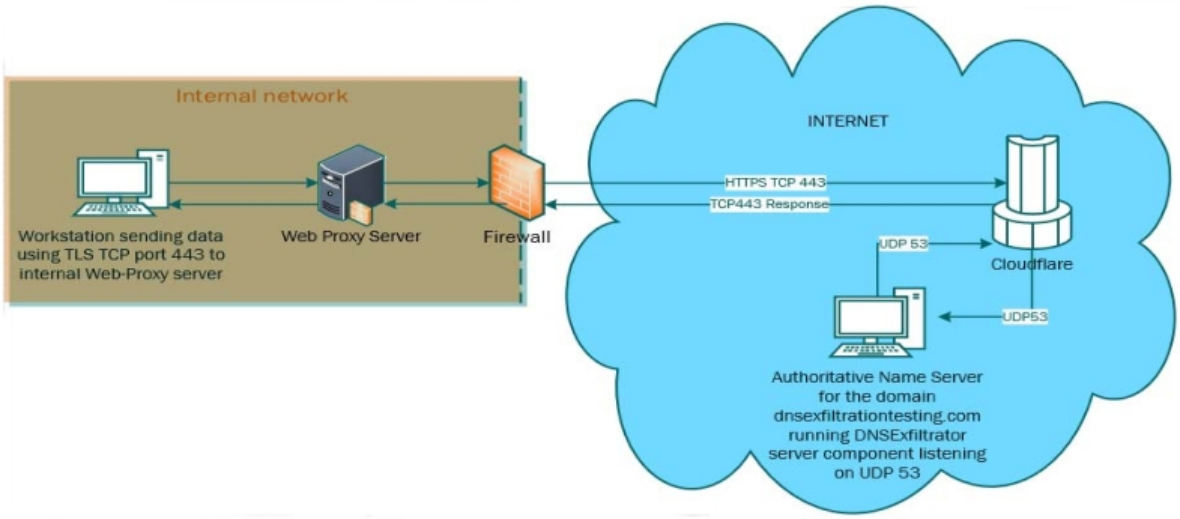
Gambar 2. Topologi SSH Tunneling

Pada saat klien mencari sebuah domain proses yang dilakukan adalah melakukan *query* ke *DNS Server* pada protokol 53. Saat ini *query* ke DNS Server dapat melalui protokol TCP 443 atau HTTPS. Namun, hal ini masih dalam uji coba sesuai usulan yang tercantum pada RFC 8484 pada bulan Oktober 2018 (Hoffman dan McManus, 2018). Beberapa perusahaan seperti Google, Cloudflare dan Mozilla ikut menguji coba usulan ini. Mozilla melalui peramban Firefox sudah menerapkan *DNS over HTTPS* (DoH) pada bagian konfigurasi jaringan. Gambar 3 menunjukan query ke *DNS Server* melalui protokol TCP 443 yang dianggap oleh *firewall* sebagai trafik HTTPS (Hoffman dan McManus, 2018).

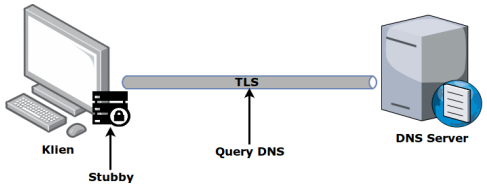
Usulan speksifikasi *DNS over Transport Layer Security* (TLS) diajukan lebih dulu dibandingkan *DNS over HTTPS* yaitu tahun 2016. Berbeda dengan *DNS over HTTPS* yang berjalan pada protokol TCP 443, DNS over TLS (DoT) berjalan pada protokol TCP 853 (Hu et al., 2016). Dalam mengimplementasi *DNS over TLS* (DoT) memerlukan *Stub Resolver* yang disebut *Stubby* yang terhubung dengan *DNS Server* publik seperti Google, Cloudflare, dan Quad9 DNS. Gambar 4 menunjukan koneksi yang terenkripsi jika jalur

1 https://play.google.com/

komunkasi TLS telah stabil (Van Heugten, 2018). Dari sisi klien Google melalui sistem operasi Android versi Pie mulai menerapakan *DNS over TLS* (DoT). Sistem operasi Android sebelum versi Pie belum tersedia fitur *DNS over TLS* (DoT) (Kline dan Schwartz, 2018).



Gambar 3. Topologi DNS over HTTPS

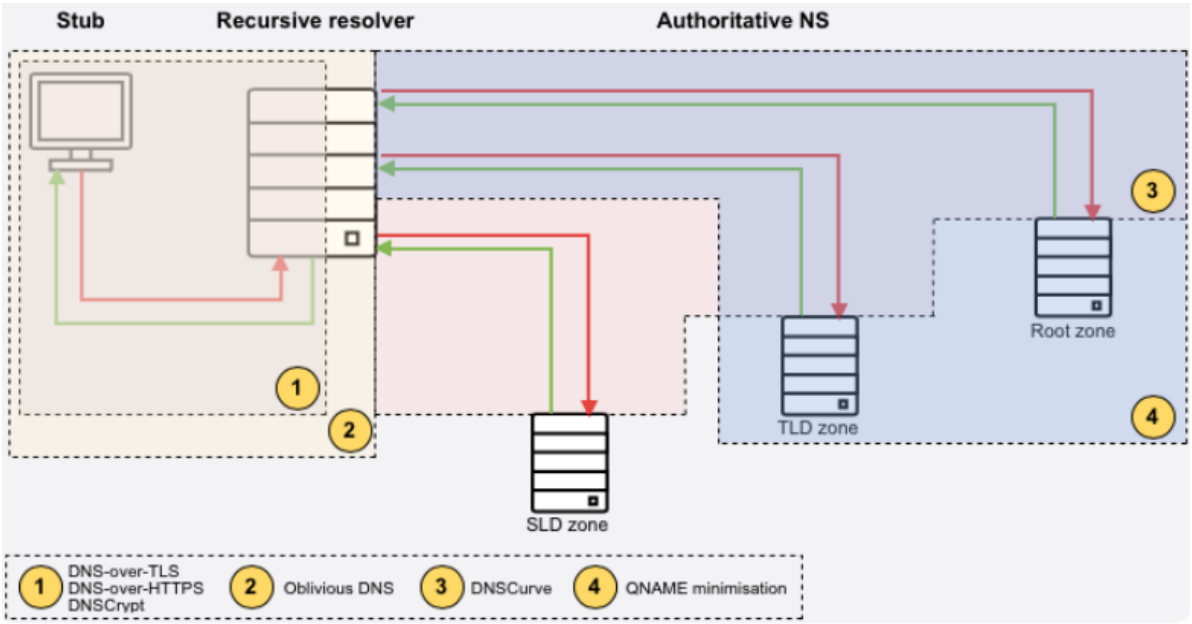


Gambar 4. Diagram DNS over TLS

DNSCrypt menggunakan protokol yang terenkripsi antara pada fase klien dengan *DNS Server/Recursive Resolver*. Fase enkripsi pada DNS terbagi menjadi dua fase. DNSScrypt merupakan fase pertama sedangkan fase kedua enkripsi antara *DNS Server* dengan Server Otoritatif. Diagram teknik DNS yang bersifat privat dapat dilihat pada Gambar 5 (Van Heugten, 2018).

The onion router atau dikenal dengan Tor merupakan teknologi pengamanan komunikasi melalui jaringan internet yang dikenalkan pada tahun 2002 melalui *mailing-list* Free Haven (Roger Dingledine, 2002). Proyek Tor memiliki tujuan desain diantaranya (Dingledine, Mathewson dan Syverson, 2004):

1. *Deployability*, desainnya dapat diterapkan pada dunia nyata.
2. *Usability*, mudah diimplementasikan pada semua platform yang biasa digunakan banyak pengguna.

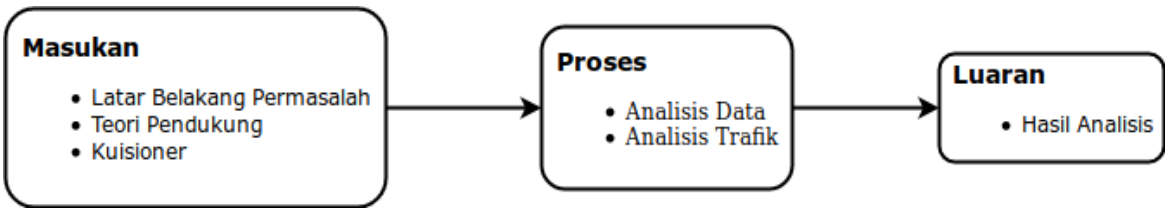


Gambar 5. Diagram Teknik DNS Bersifat Privat

3. *Flexibility*, memiliki speksifikasi yang dan fleksibel sehingga memudahkan penlitian lebih lanjut.
4. *Simple Design*, rancangan protokol dan parameter keamanan harus mudah dipahami dengan baik.

3. METODE PENELITIAN

Pada penelitian ini terbagi menjadi tiga tahapan, **Masukan** berupa latar belakang permasalahan yang terjadi di sekitar peneliti, mempelajari teori pendukung dan membagikan kuisioner, **Proses** melakukan analisis hasil dari kuisioner yang telah disebarluaskan dan menganalisis trafik jaringan, dan **Luarannya** berupa hasil analisis terkait proteksi komunikasi pada jaringan internet. Adapun tahapan tersebut dapat dilihat pada Gambar 6.



Gambar 6. Tahapan Penelitian

Dalam proses analisis trafik jaringan melakukan analisis terhadap aliran paket data yang melewati router pada suatu jaringan. Tahapan ini juga biasa disebut juga *packet analyzer* yang memungkinkan memonitor dan menangkap informasi dari paket data seperti: kata sandi dari *File Transfer Protocol*, kata sandi dari Telnet, konfigurasi router, trafik dari *Domain Name System*, trafik surat eletronik, trafik dari web, dan sesi percakapan *Instant Messenger* (Anu dan Vimala, 2017). Pada penelitian ini hanya fokus mengamati trafik dari *Domain Name System* dan aliran informasi situs web.

4. ANALISIS DAN PEMBAHASAN

4.1 Hasil Survei

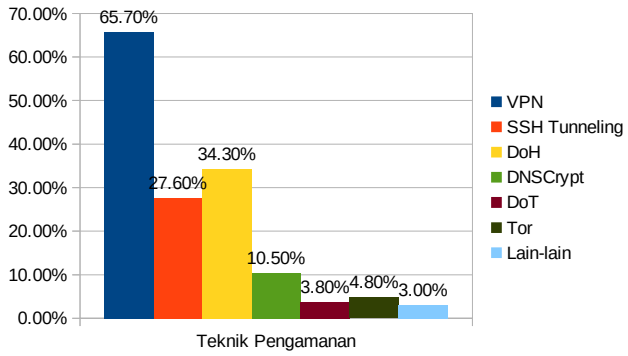
Proses penyebaran kuisioner dilakukan sebelum kejadian pembatasan *Instant Messenger* dan Sosial Media oleh Kementerian Komunikasi dan Informatika (Kementerian Komunikasi dan Informatika, 2019b) (Kementerian Komunikasi dan Informatika, 2019a). Penyebaran kuisioner dimulai tanggal 30 Aprill 2019 hingga 25 Mei 2019 dengan total responden sejumlah 203 responden yang tersebar di seluruh Indonesia karena kuisioner disebarluaskan secara daring. Sasaran responden dengan batasan yaitu responden yang sedang menempuh studi dari jenjang Sekolah Menengah Pertama atau setara sampai dengan Doktoral. Umur pada survei ini tidak menjadi batasan karena pada jenjang pendidikan Sarjana hingga Doktoral umurnya sangat variatif. Pada kuisioner tidak terdapat pertanyaan yang bersifat pribadi seperti Nama, Alamat Lengkap, Tempat Lahir, Tanggal Lahir, Surat Elektronik, dan Nomor Ponsel. Hal ini untuk menjaga dan menghormati responden terkait informasi pribadi.

Responden berdasarkan jenis kelamin didominasi oleh perempuan dengan persentase 54,2% sedangkan laki-laki sebesar 45,8%. Berdasarkan jenjang pendidikan responden terbesar didominasi Sarjana/Diploma sebesar 65,6%, selanjutnya jenjang pendidikan SMA/SMK/MAN sebesar 29,6%. Alamat sekolah atau perguruan tinggi dikategorikan berdasarkan provinsi atau setingkatnya. Adapun asal sekolah atau perguruan tinggi terbesar responden berasal dari Pemerintah Daerah Istimewa Yogyakarta sebesar 48,8% dan Provinsi Jawa Tengah sebesar 26,1%.

Perangkat yang digunakan untuk mengakses internet didominasi menggunakan ponsel dengan persentase 95,6%. Hal ini juga berbanding lurus dengan hasil survei yang dilakukan oleh APJII dengan obyek pertanyaan yang serupa bahwa pengguna internet di Indonesia lebih banyak menggunakan ponsel yang sebesar 93,9% (Asosiasi Penyelenggara Jasa Internet, 2019). Responden pengguna internet menyatakan terganggu adanya iklan pada ponsel sebesar 93,1%. Selain itu responden menyatakan tidak mengetahui bahwa adanya proses MITM saat mengakses internet. MITM merupakan serangan dengan posisi penyerang memungkinkan mengambil alih komunikasi yang berlangsung antara dua atau lebih saluran. Hal ini seorang penyerang dapat "mendengar" lalu lintas antara korban dan server pada subnet jaringan yang sama (Chordiya, Majumder dan Javaid, 2018).

Walaupun responden banyak tidak mengetahui adanya proses MITM saat mengakses internet tetapi perbandingan responden yang memasang aplikasi tambahan untuk mengamankan komunikasi tidak terlalu besar sekitar 52.8% responden yang tidak memasang memasang aplikasi tambahan. Apalagi saat kejadian pembatasan *Instant Messenger* dan Sosial Media pada tanggal 22 hingga 25 Mei 2019 pengguna internet mulai memasang aplikasi tambahan untuk mengamankan jalur komunikasi dalam rangka mengalihkan sistem sensor. Adapun responden yang menggunakan atau memasang aplikasi tambahan untuk mengamankan komunikasi

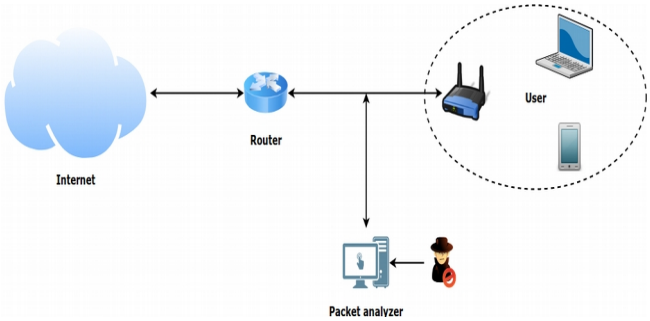
saat akses internet dapat dilihat pada Gambar 7. Pengguna VPN paling tinggi sebesar 65,7% selanjutnya *DNS over HTTPS* 34,3%, *SSH Tunneling* 27,6%, DNSCrypt 10,5%, Tor 4,8%, dan *DNS over TLS* 3,8%.



Gambar 7. Grafik Persentase Teknik Pengamanan

4.2 Hasil Analisis Trafik

Peranti lunak yang digunakan pada *packet analyzer* adalah tcpdump yang berjalan diatas sistem operasi GNU/Linux dan CapLoader yang berjalan diatas sistem operasi MS Windows. Pengguna mengakses beberapa domain yang telah diblokir oleh Kementerian Komunikasi dan Informatika, TRUST+ (Kementerian Komunikasi dan Informatika, 2019). Teknik pengamanan yang digunakan untuk mengakses alamat tersebut menggunakan: VPN, SSH Tunneling, *DNS over HTTPS*, DNSCrypt, *DNS over TLS*, dan Tor. Gambar 8 menunjukan topologi dalam proses *packet analyzer* untuk memonitor dan menangkap informasi paket data yang melewati router.



Gambar 8. Analisis Trafik Jaringan

Pengujian pengamanan akses internet menggunakan aplikasi VPN gratis yang terinstall pada ponsel cerdas bersistem operasi Android. Aplikasi VPN gratis yang didapatkan dari Google Play Store. Dengan menggunakan VPN tersebut hasilnya dapat mengakses suatu situs tanpa terdeteksi oleh sistem sensor. Gambar 9 menunjukan *IP Address* dan *Hostname* situs web tujuan tidak terdeteksi oleh sistem sensor karena informasi *IP Address* dan *Hostname* telah dibungkus oleh aplikasi VPN untuk dikirimkan ke *VPN Server* yang tidak memiliki sistem sensor.

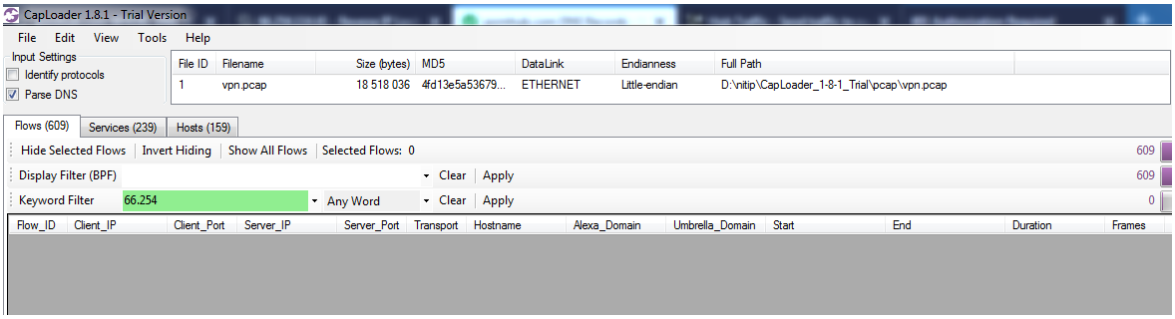
Berbeda dengan pengujian VPN, pada pengujian *SSH Tunneling* menggunakan komputer bersistem operasi Linux dengan memanfaatkan aplikasi *SSH Client* yang terhubung dengan *SSH Server*. Format penggunaan *SSH Tunneling* adalah `ssh -D 1234 user@ssh-server -p 22`. Selanjutnya pada konfigurasi jaringan peramban web diarahkan proxy menggunakan metode SOCK ke localhost port 1234. Hasil pengujian serupa dengan VPN, *SSH Tunneling* melakukan teknik pembungkusan informasi *IP Address* dan *Hostname* melalui protokol SSH. Jadi sistem sensor tidak dapat mendeteksi sebuah informasi *IP Address* dan *Hostname* yang masuk dalam daftar hitam, seperti tampak pada Gambar 10.

Untuk pengujian pengamanan akses internet menggunakan metode *DNS over HTTPS* memanfaatkan ponsel cerdas bersistem operasi yang telah terinstall aplikasi Intra yang dapat diunduh dari Google Play Store dan menggunakan peramban web Mozilla Firefox yang telah mendukung metode *DNS over HTTPS*. Hasil pengujian menggunakan *DNS over HTTPS* bahwa sistem sensor tidak mendeteksi *DNS Query* jadi trafik yang terlihat hanya *IP Address*, seperti tampak pada Gambar 11.

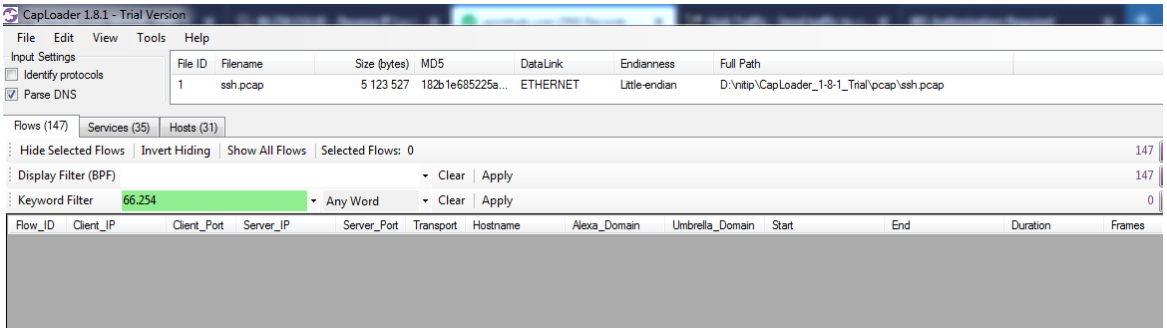
DNSCrypt diuji menggunakan komputer bersistem operasi GNU/Linux yang menjalankan layanan DNSCrypt-Proxy. Pada aplikasi peramban web tidak ada konfigurasi apapun terkait dengan konfigurasi proxy seperti pada metode *SSH Tunneling*. Pada DNSCrypt hasilnya serupa dengan *DNS over HTTPS* sistem sensor tidak dapat mendeteksi *DNS Query* yang masuk dalam daftar hitam, seperti yang ditunjukan pada Gambar 12.

Gambar 13 tampak seperti hasil analisis *DNS over HTTPS* dan DNSCrypt, *DNS Query* dari daftar hitam tidak terdeteksi oleh sistem sensor. Pengujian *DNS over TLS* serupa dengan *DNS over HTTPS* yang menggunakan ponsel cerdas. Ponsel cerdas yang digunakan adalah ponsel cerdas bersistem operasi Android versi Pie yang telah mendukung teknologi *DNS over TLS*. *Server* yang digunakan adalah dns.google.

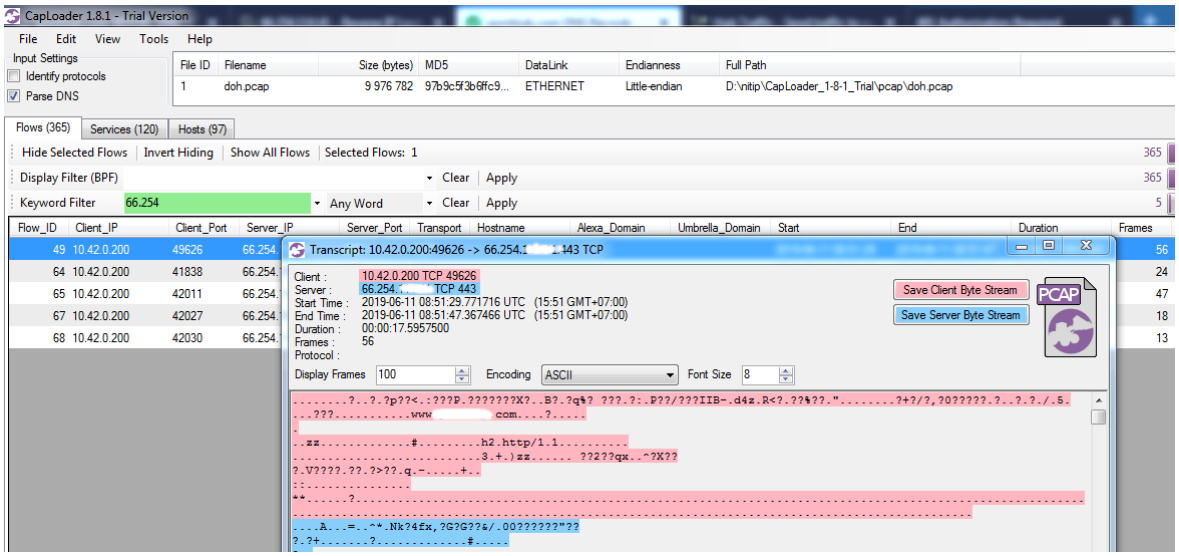
Walaupun hasil pengujian Tor seperti VPN dan *SSH Tunneling* yang tampak pada Gambar 14, Tor memiliki rancangan berbeda yaitu fokus pada komunikasi anonim. Sehingga pihak klien tidak mengetahui *Tor Server* yang dituju bahkan pemilihannya dapat secara acak termasuk alur *routing*-nya. Proses pengujian Tor menggunakan ponsel cerdas bersistem operasi Android yang terinstall *Tor Client* dan Orfox sebagai peramban web.



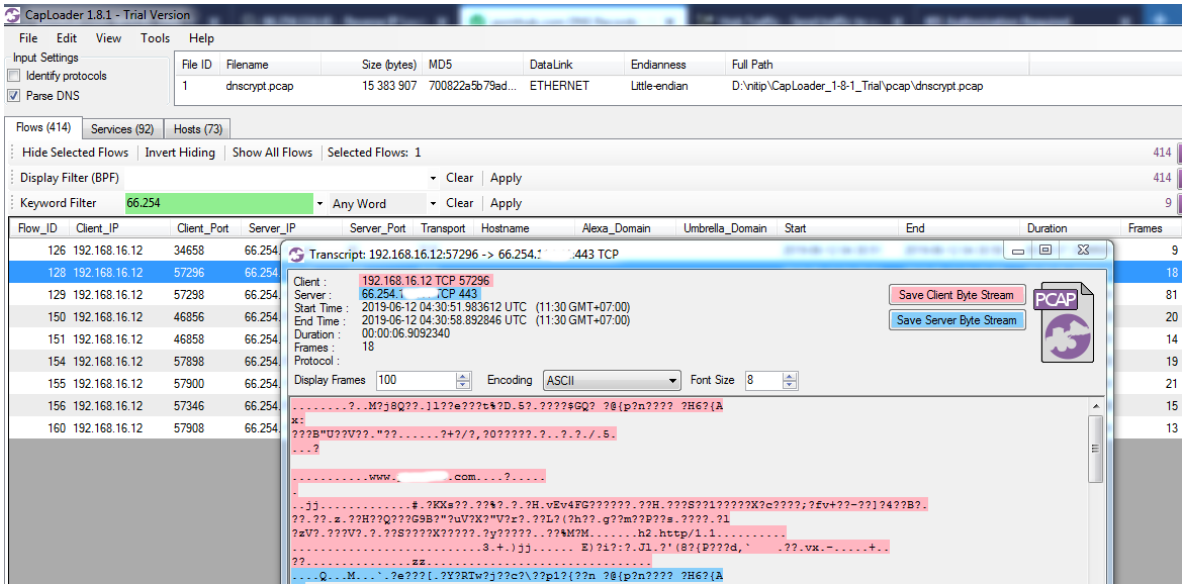
Gambar 9. Analisis Trafik VPN



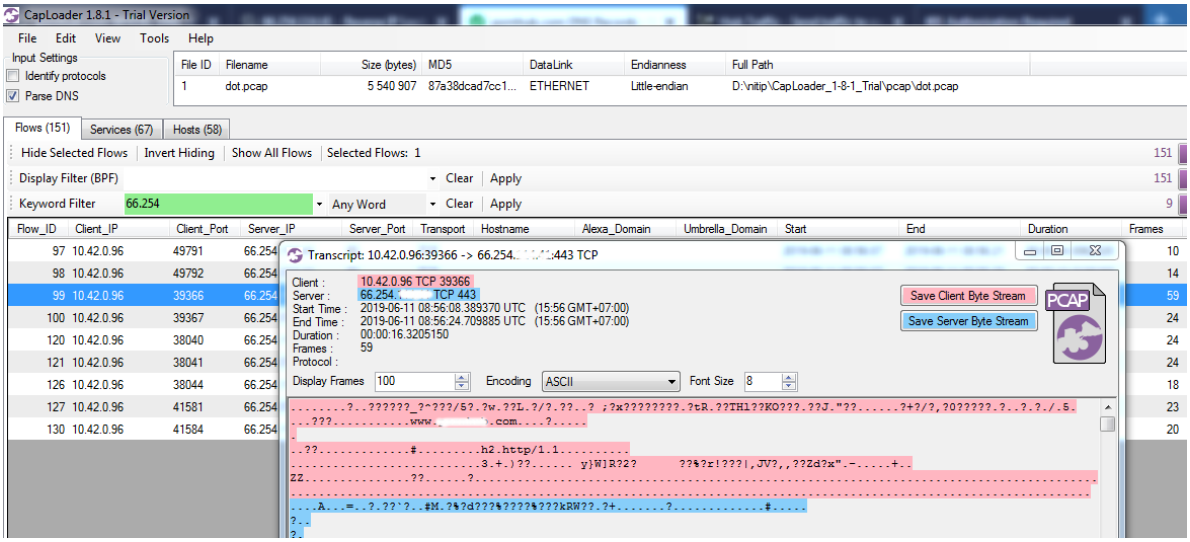
Gambar 10. Analisis Trafik *SSH Tunneling*



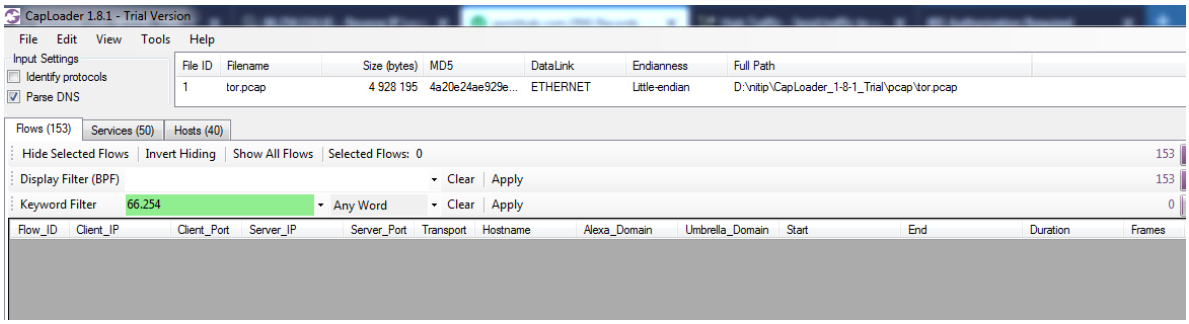
Gambar 11. Analisis Trafik *DNS over HTTPS*



Gambar 12. Analisis Trafik DNSCrypt



Gambar 13. Analisis Trafik *DNS over TLS*



Gambar 14. Analisis Trafik Tor

5. KESIMPULAN

Berdasarkan hasil pengujian bahwa metode pengamanan akses internet menggunakan VPN, SSH Tunneling, *DNS over HTTPS, DNS over TLS*, DNSCrypt, dan Tor dapat menghindari sistem sensor. Menggunakan metode VPN, SSH Tunneling dan Tor alamat tujuan berupa *IP Address* dan *Hostname* tidak terdeteksi oleh sistem sensor sedangkan metode *DNS over HTTPS, DNS over TLS* dan DNSCrypt yang diamankan adalah *DNS Query*

walaupun *IP Address* masih dapat terlacak. Sistem sensor saat ini yang diterapkan di Indonesia menggunakan metode penyaringan berbasis *Domain Name System* dengan mencatat alamat-alamat yang bersifat negatif yang dimasukan ke dalam daftar hitam. Oleh sebab itu metode *DNS over HTTPS, DNS over TLS* dan DNSCrypt tetap lolos dari pantauan sistem sensor pemerintah Indonesia.

DNS over HTTPS, DNS over TLS ataupun DNSCrypt dirancang untuk melindungi serangan *Man-in-the-Middle* oleh pihak-pihak tertentu. Sehingga tujuan penggunaan metode *DNS over HTTPS, DNS over TLS* ataupun DNSCrypt memiliki tujuan diantaranya adalah melindungi penyisipan kode-kode jahat, menghalau iklan-iklan yang menggangu, melindungi pornografi, dan sebagainya. Jadi pemasangan aplikasi pengaman akses internet bukan untuk menghindari sistem sensor.

DAFTAR PUSTAKA

Asosiasi Penyelenggara Jasa Internet Indonesia and Teknopreneur Indonesia, 2018. Penetrasi & Perilaku Pengguna Internet Indonesia - Survey 2017. Jakarta.

Asosiasi Penyelenggara Jasa Internet, 2019. "Penetrasi dan Profil Perilaku Pengguna Internet Indonesia 2018". Jakarta.

Masyarakat Telematika Indonesia, 2018. Survey 2017: Wabah Hoax Nasional.

Kementerian Komunikasi dan Informatika, 2019. Pembatasan Sebagian Fitur Platform Media Sosial dan Pesan Instan. [Online]. Available: https://kominfo.go.id/content/detail/18868/siaran-pers-no-106hmkominfo052019-tentang-pembatasan-sebagian-fitur-platform-media-sosial-dan-pesan-instan/0/siaran_pers. [Accessed: 22-May-2019].

Kementerian Komunikasi dan Informatika, 2019. Normalisasi Fitur Platform Media Sosial dan Pesan Instan. [Online]. Available: https://www.kominfo.go.id/content/detail/18918/siaran-pers-no-107hmkominfo052019-tentang-normalisasi-fitur-platform-media-sosial-dan-pesan-instan/0/siaran_pers. [Accessed: 25-May-2019].

M. Ikram, N. Vallina-Rodriguez, S. Seneviratne, M. A. Kaafar, and V. Paxson, 2016. An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps," in *Proceedings of the 2016 ACM on Internet Measurement Conference - IMC '16*, pp. 349–364.

M. Lewis, 2006. *Comparing, Designing, and Deploying VPNs*. Indianapolis, Indiana: Cisco Press.

A. S. Tanenbaum and D. J. Wetherall, 2011. *Computer Networks*, Fifth Edit. Prentice Hall..

O. W. Purbo, 2009. Virtual Private Network (VPN) sebagai alternatif Komunikasi Data Pada Jaringan Skala Luas (WAN).

S. Kent and R. Atkinson, 1998. RFC2406: IP Encapsulating Security Payload.

D. Hariyadi, I. A. Subhan, and A. R. J. Vanca, 2018. Model Pengujian Celah Keamanan Bug Host pada Layanan Promosi Operator Seluler. *J. INTEK Univ. Muhammadiyah Purworejo*, vol. 1, pp. 1–6.

P. Hoffman and P. McManus, 2018. RFC 8484: DNS Queries over HTTPS (DoH).

Z. Hu, L. Heidemann, A. Mankin, D. Wessels, and P. Hoffman, 2018. RFC 7858: Specification for DNS over Transport Layer Security (TLS).

J. H. C. Van Heugten, 2018. Privacy analysis of DNS resolver solutions," Amsterdam.

E. Kline and B. Schwartz, 2018. Android Developers Blog: DNS over TLS support in Android P Developer Preview. [Online]. Available: https://android-developers.googleblog.com/2018/04/dns-over-tls-support-in-android-p.html. [Accessed: 25-May-2019].

Roger Dingledine, 2002. pre-alpha: run an onion proxy now!," *Free Haven*. [Online]. Available: https://archives.seul.org/or/dev/Sep-2002/msg00019.html. [Accessed: 23-May-2019].

R. Dingledine, N. Mathewson, and P. Syverson, 2004. Tor: The Second-Generation Onion Router Roger.

P. Anu and S. Vimala, 2017. A Survey on Sniffing Attacks on Computer Networks. *Proc. 2017 Int. Conf. Intell. Comput. Control. I2C2 2017*, pp. 1–5.

A. R. Chordiya, S. Majumder, and A. Y. Javaid, 2018. Man-in-the-Middle (MITM) Attack Based Hijacking of HTTP Traffic Using Open Source Tools. *2018 IEEE Int. Conf. Electro/Information Technol.*, pp. 438–443.

Kementerian Komunikasi dan Informatika, "TRUST+™ Positif (Internet Sehat dan Aman)." [Online]. Available: https://trustpositif.kominfo.go.id/. [Accessed: 06-Jan-2019].