**Perbandingan Trafic Tapping Menggunakan TOR dan Tools Lain**



Oleh:

Nam : Muhammad Taufik Hidayat

NIM : 09040581721001

Prodi : TKJ4

Mata Kuliah : Keamanan Jaringan Komputer

Dosen Pengampu : Deris Stiawan, M.T., Ph.D.

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS SRIWIJAYA**

**2019**

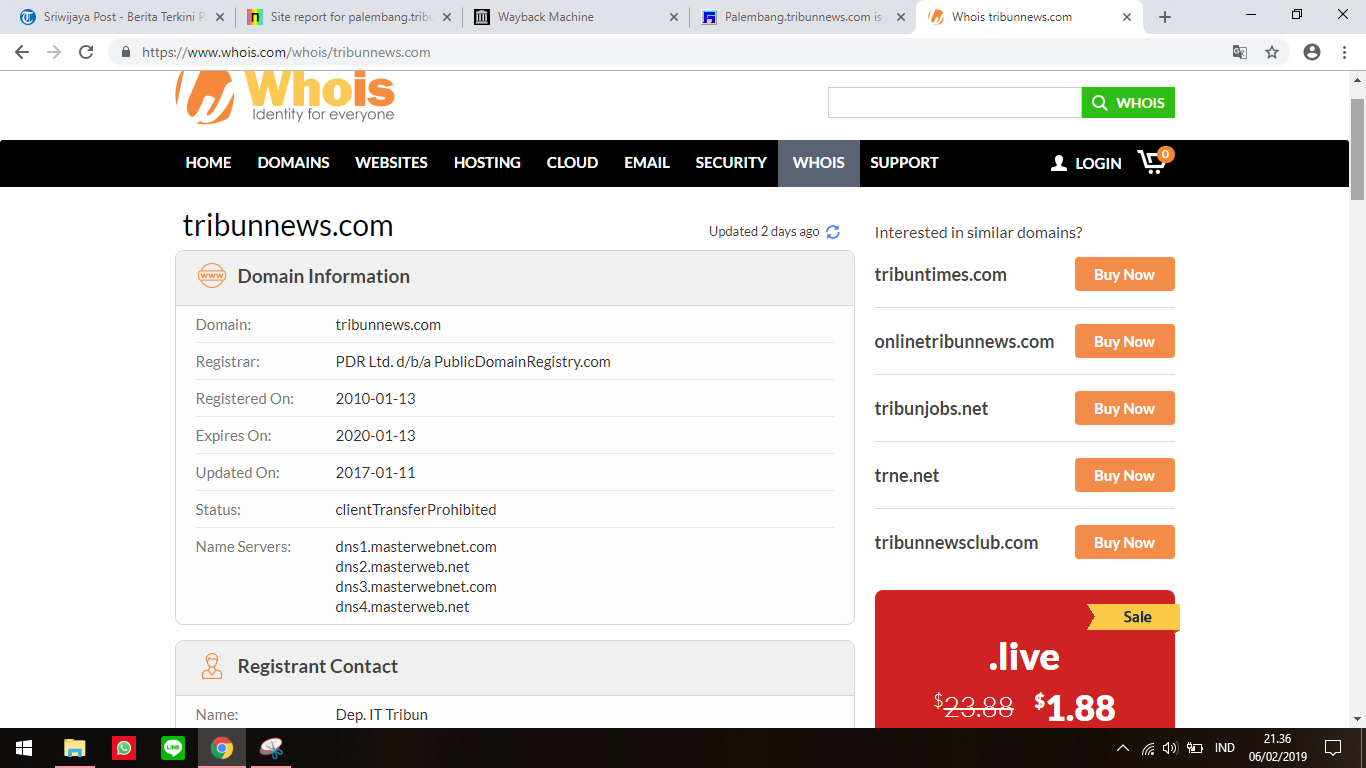
**Pengenalan**

**1. Wireshark** adalah salah satu dari sekian banyak tool Network Analyzer yang banyak digunakan oleh Network Administrator untuk menganalisa kinerja jaringannya dan mengontrol lalu lintas data di jaringan yang Anda kelola. Wireshark menggunakan interface yang menggunakan Graphical User Interface (GUI).

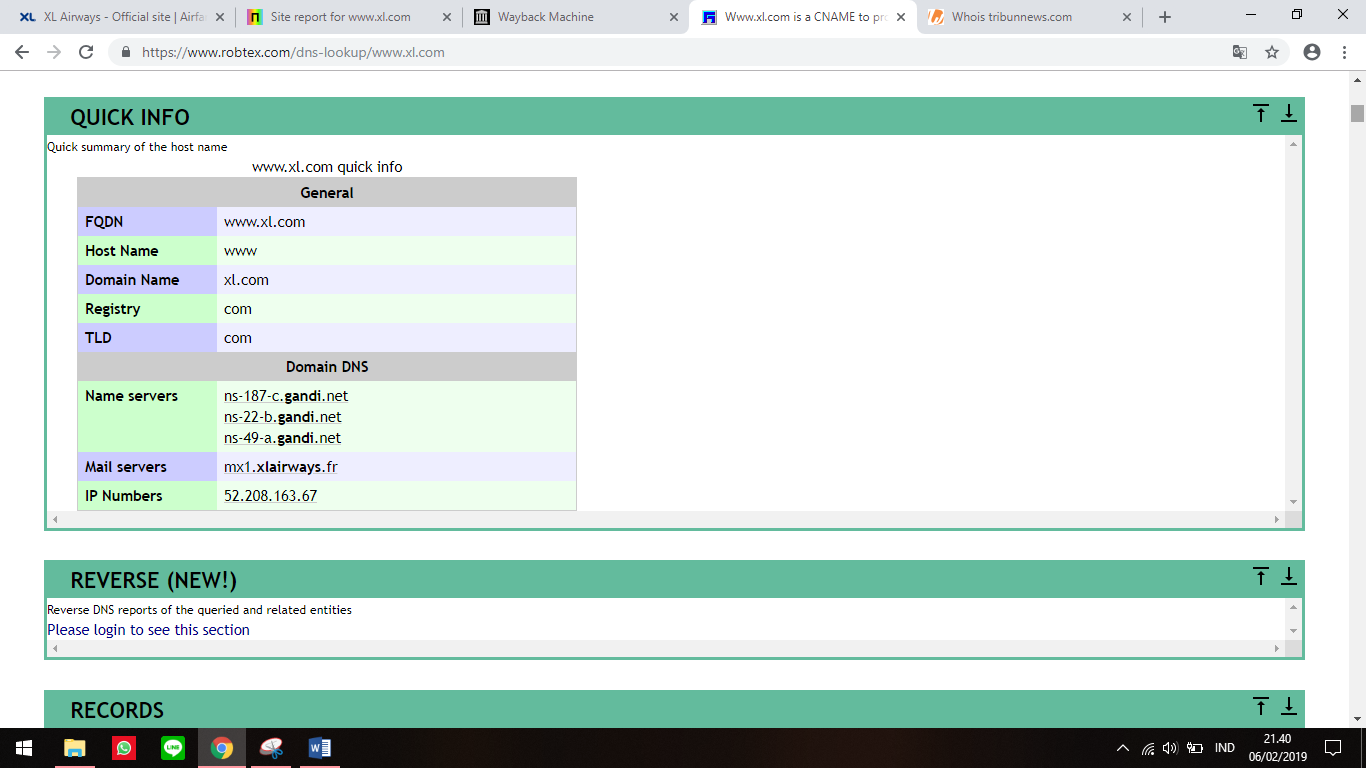
**2. Tor Browser** adalah versi Mozilla Firefox yang termutakhir dan dioptimalkan untuk privasi. ... Tidak seperti peramban lainnya, **Tor Browser**: menyediakan anonimitas daring dengan menyembunyikan alamat IP pengguna. menembus sensor daring dengan memampukan pengguna untuk mengakses situs web dan/atau halaman web yang diblokir.

**TOOLS-TOOLS YANG DIGUNAKAN**

Whois **adalah** suatu prosedur untuk mendapatkan informasi mengenai sebuah domain. Informasi yang bisa di dapat meliputi siapa pemilik Domain, dimana alamatnya, no telepon, alamat email, kapan domain ini di daftarkan dan kapan domain ini akan expire.

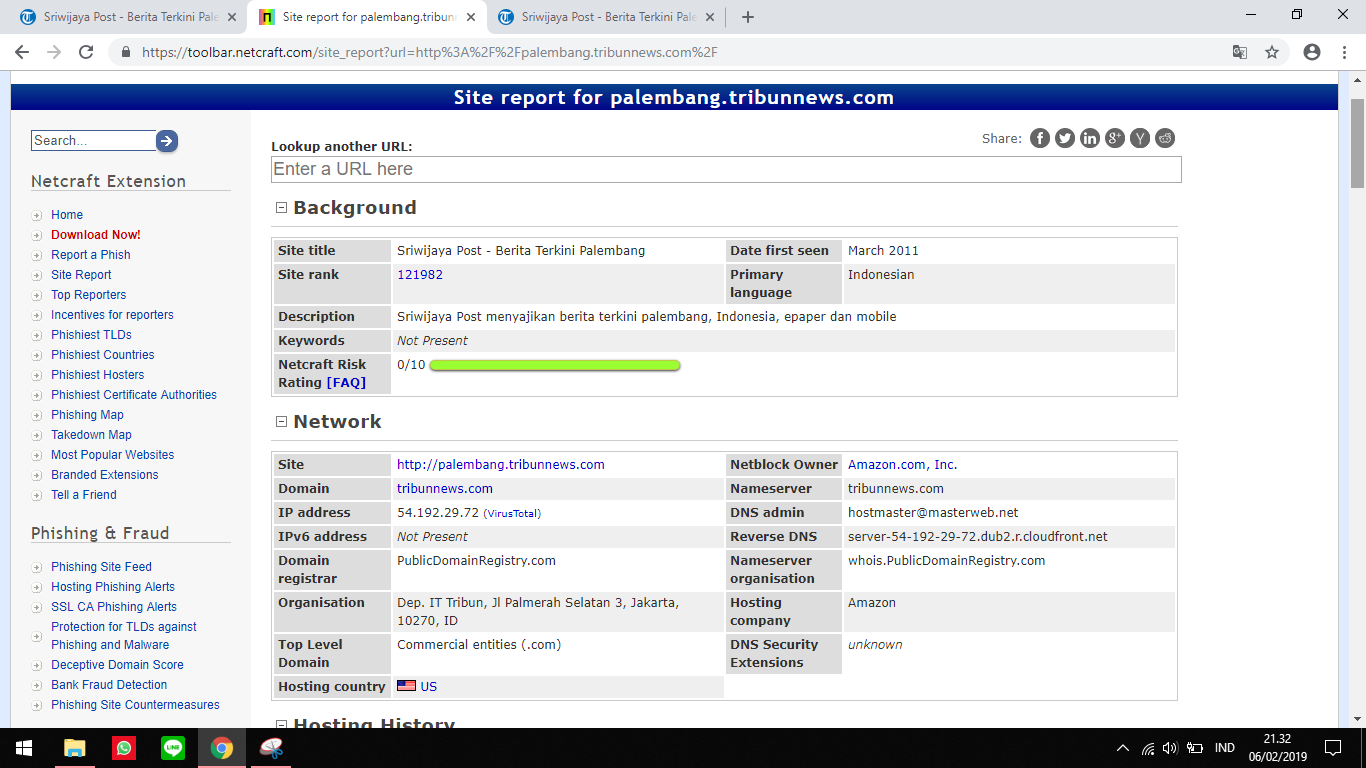


Robtex adalah tools foot printing sama seperti whois namun lebih prefer kepada alamat domain dan host name yang digunakan oleh pemilik website tersebut.



Netcraft adalah perusahaan penyedia layanan Internet yang berbasis di Bath, Inggris. Pendapatan yang diperoleh oleh Netcraft bersumber dari:

* Penyedia layanan keamanan Internet yang mencakup layanan *anti-fraud* dan *anti-phishing*, pengetesan aplikasi dan lain-lain.
* Menyediakan data-data untuk penelitian pada berbagai aspek di Internet. Netcraft telah menjelajah Internet sejak 1995 dan memiliki kewenangan pada *market share* dari *web server*, sistem operasi, *hosting providers*, ISP, transaksi terenkripsi, bisnis secara elektronik, bahasa-bahasa *scripting* dan teknologi konten di Internet.
* Biaya iklan pada situs Netcraft.

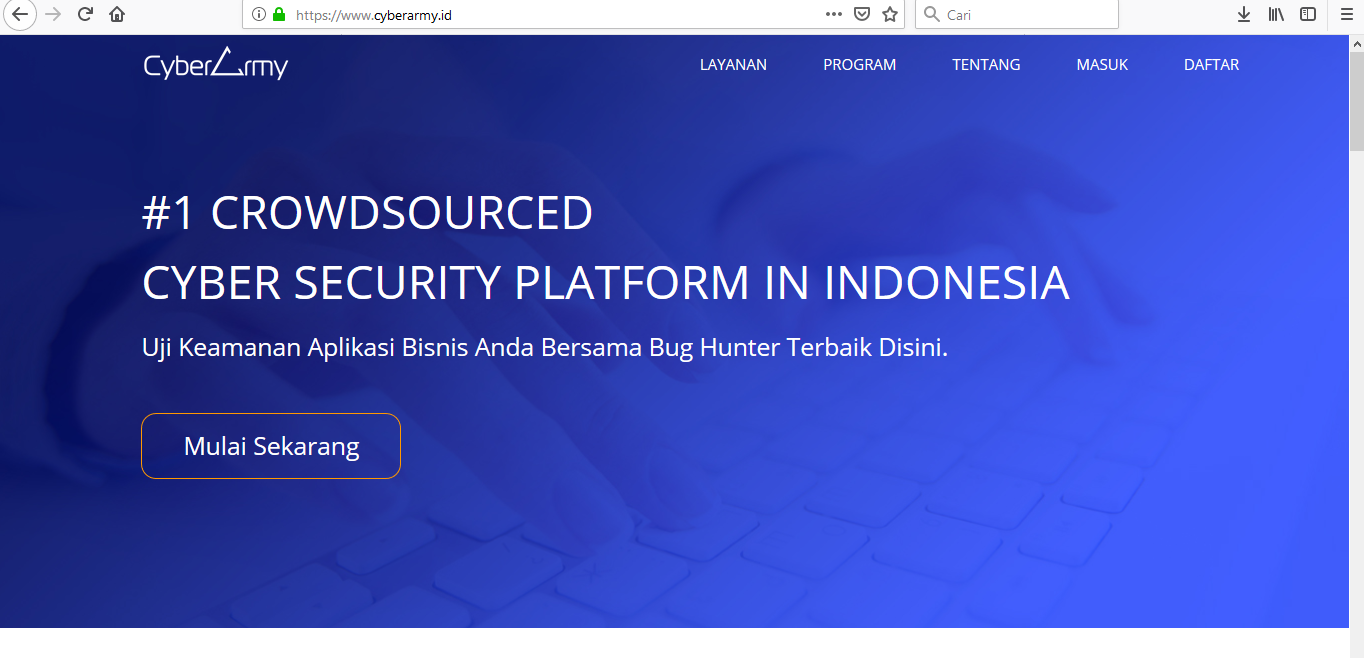


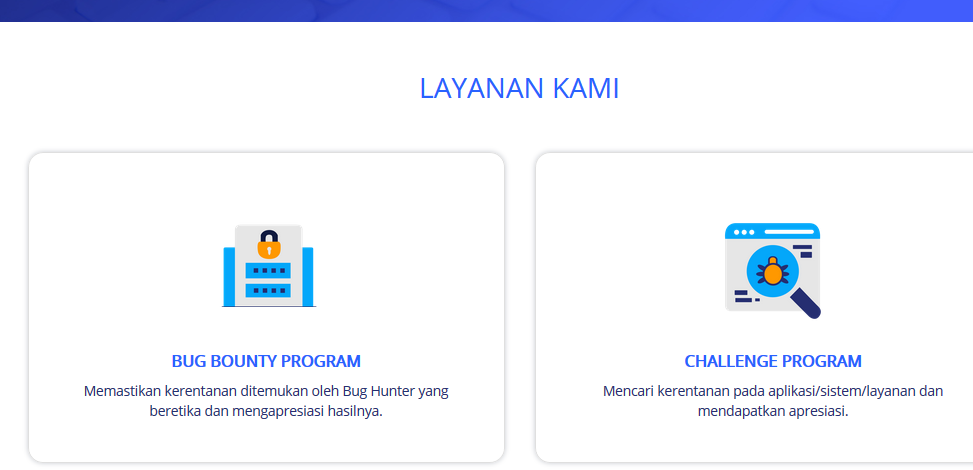
**CYBER ARMY INDONESIA**

1.Cyber Army Indonesia (CyberArmyID) merupakan platform pertama di Indonesia yang mengumpulkan dan memvalidasi laporan dari rekan-rekan Peretas (disebut sebagai Bug Hunter) mengenai kerentanan yang ada pada suatu Organisasi. Selanjutnya, pihak Organisasi akan menerima laporan tersebut untuk ditindaklanjuti, dan kemudian memberikan apresiasi kepada Bug Hunter yang melaporkannya.

CyberArmyID juga berperan sebagai salah satu Pusat Koordinasi Kerentanan dari sektor publik yang hasilnya nanti akan dapat menjadi acuan Keamanan Siber dan Informasi yang terintegrasi di Indonesia.

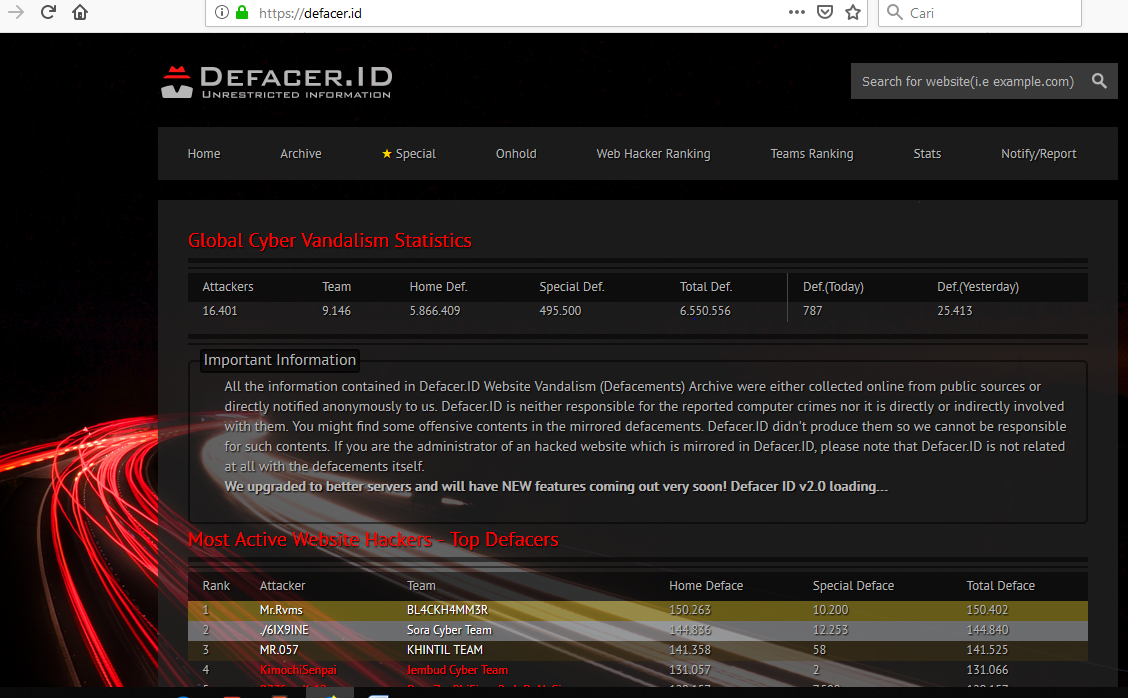
Cyber armyID juga sebagai wadah untuk perusahaan-perusaahaan untuk menguji keamanan server website dan networking pada perusahaan tersebut atau juga dikenla juga dengan pentest

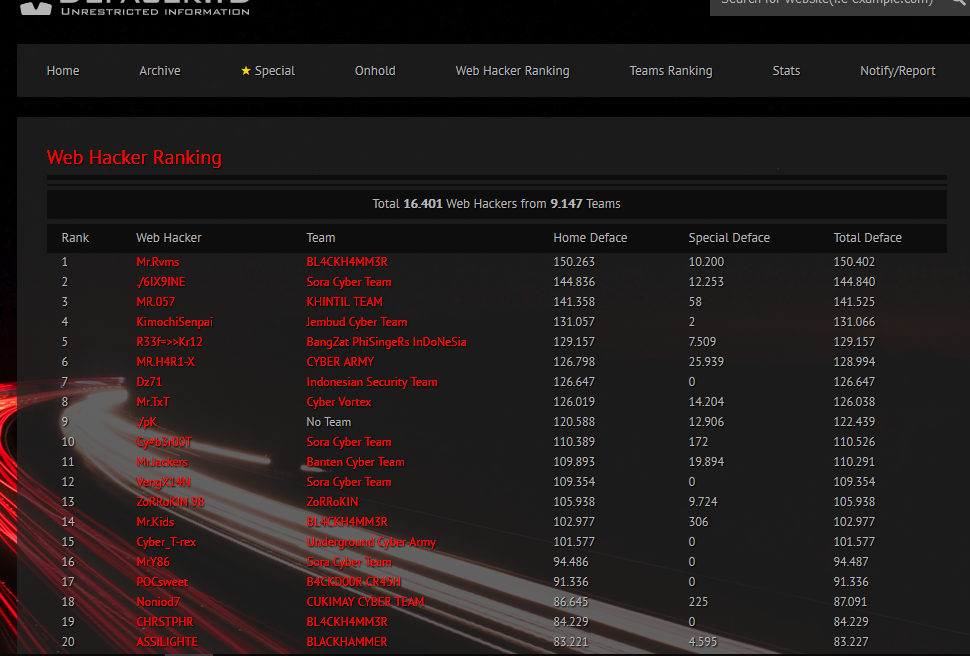




**DEFACER ID**

Defacer pada umumnya adalah orang iseng yang ssedang mecoba mencari tahu baik dari segi ilmu kemampuan, dan jati diri. Kebiasaan yang mudah diketahui dari mereka adalah mereka gemar merubah tampilan utama website, menggunakan kelemahan atau kecacatan dalam sebuah program. Defacer umumnya tidak begitu memahami tentang level pemrograman, mereka lebih sering memahami tenatng kinerja sebuah webserver beserta script yang ada didalamnya. Defacer.id dikenal didunia karena kemampuan nya merubah tampilan website secara ilegal dan juga banyaknya website yang telah diretas hingga ribuan website.





**CVE MITRE**

Dokumentasi MITER Corporation mendefinisikan Pengidentifikasi CVE (juga disebut "nama CVE", "nomor CVE", "CVE-IDs", dan "CVEs") sebagai pengidentifikasi umum yang unik untuk kerentanan keamanan informasi yang diketahui publik dalam paket perangkat lunak yang dipublikasikan untuk umum. Secara historis, pengidentifikasi CVE memiliki status "kandidat" ("CAN-") dan kemudian dapat dipromosikan menjadi entri ("CVE-"), namun praktik ini berakhir beberapa waktu yang lalu dan semua pengidentifikasi sekarang ditetapkan sebagai CVE. Penugasan nomor CVE bukan jaminan bahwa itu akan menjadi entri CVE resmi (misalnya CVE mungkin ditugaskan secara tidak tepat untuk masalah yang bukan kerentanan keamanan, atau yang menduplikasi entri yang ada).

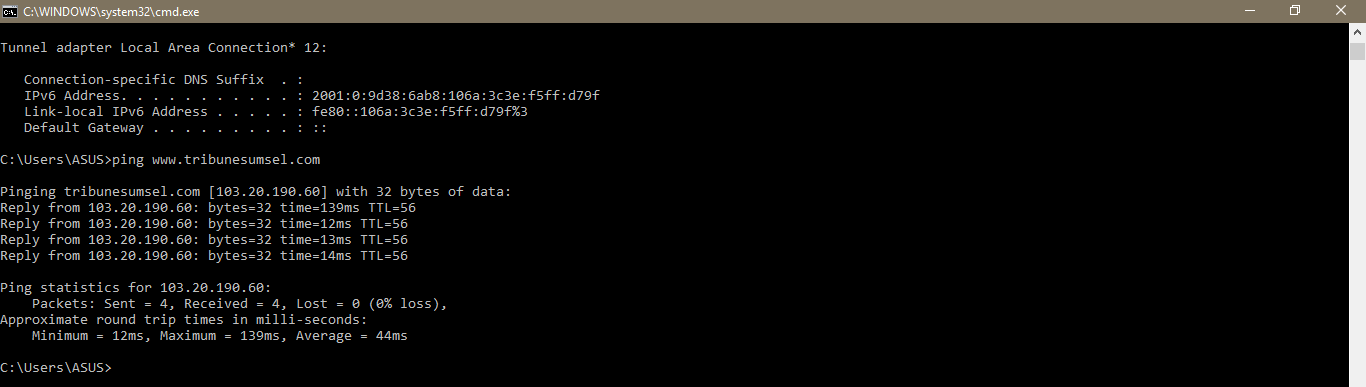
****

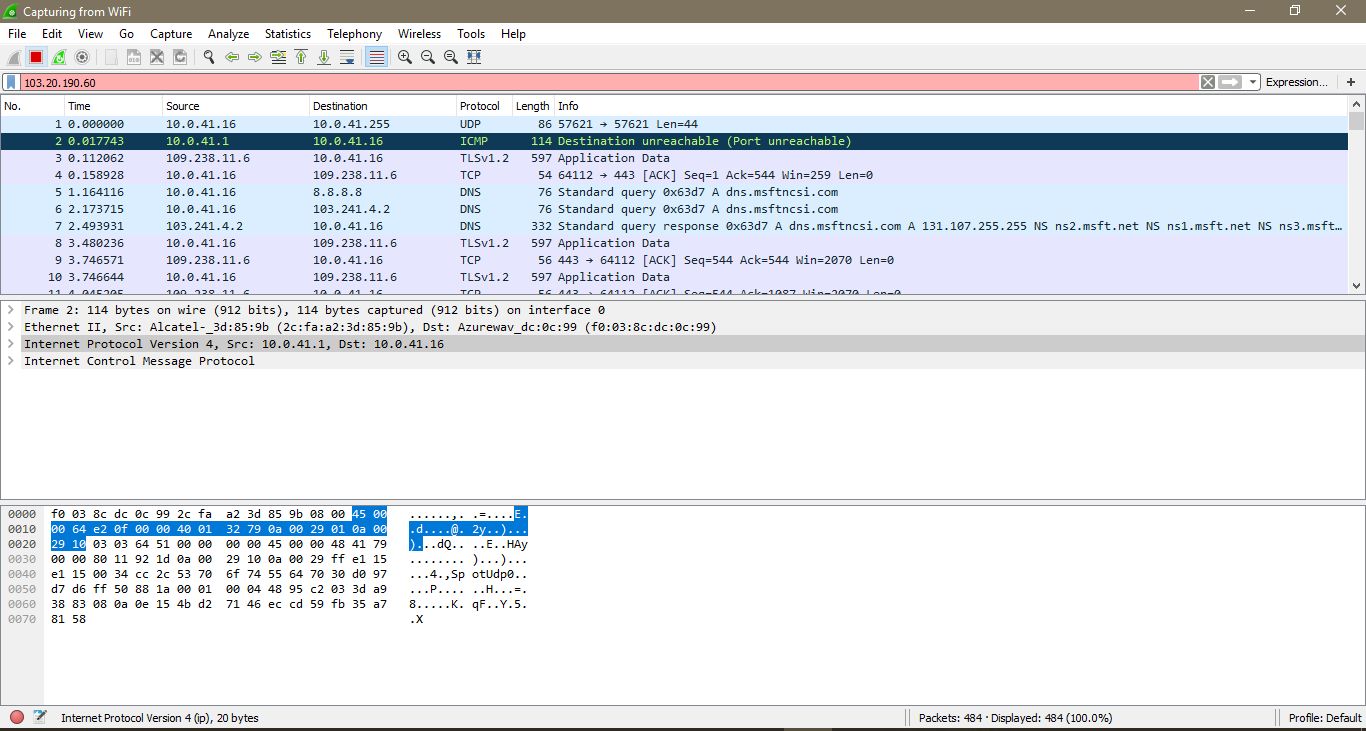
Dirty COW ( Dirty copy-on-write ) adalah kerentanan keamanan komputer untuk kernel Linux yang mempengaruhi semua sistem operasi berbasis Linux termasuk Android yang menggunakan versi lama dari kernel Linux.



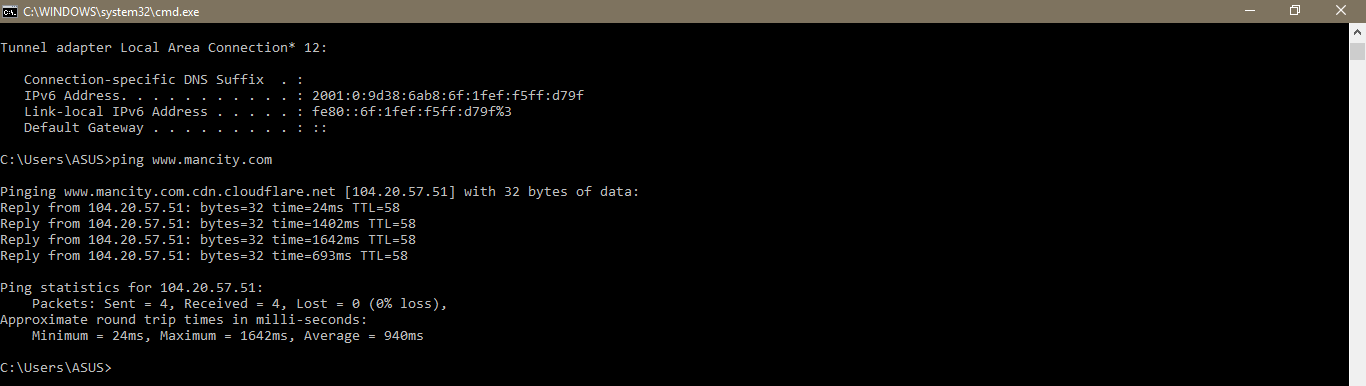
Perbedaan

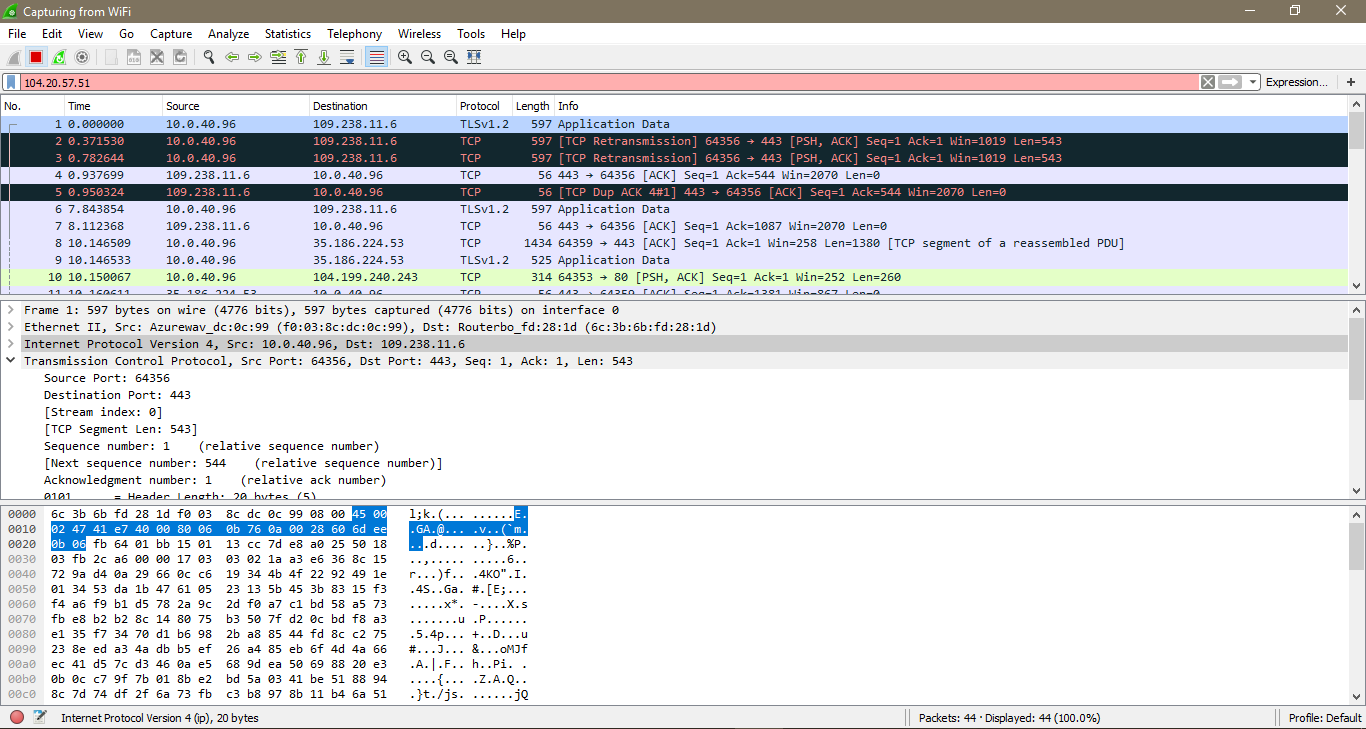
1. Jika kita menggunakan browser biasa lalu membuka wire shark masukan ip yang kita tuju di command wireshark dan hasilnya akan seperti ini, bisa kita lihat ip source dan ip destinationnya sama seperti yang ada pada command prompt. Port yang digunakan ialah port http(hypertext language)





2. Jika kita menggunakan tor browser ip yang kita gunakan di command prompt akan berbeda dengan hasil di wireshark, karena tor sendiri menyembunyikan ip kita lalu menginputkannya dengan ip orang lain sehingga kita tidak terjamah oleh situs yang kita kunjungi. Inilah yang membedakan browser biasa dan tor browser





2. TOR BROWSER digunakan untuk membuka situs situs yang telah di blokir oleh kominfo tapi agak sedikit lemot pada search engine sedangkan browser biasa cepat dalam melakukan search engine dan hanya bisa membuka situs situs yang umum, dan tidak bisa membuka situs situs yang yang telah di blokir