**VISUALISASI PCAP PAKET WEB BROWSING DAN VIDEO STREAMING DENGAN WIRESHARK**

****

Disusun oleh :

Cynthia Caroline 09011281520101

**Universitas Sriwijaya**

**Indralaya**

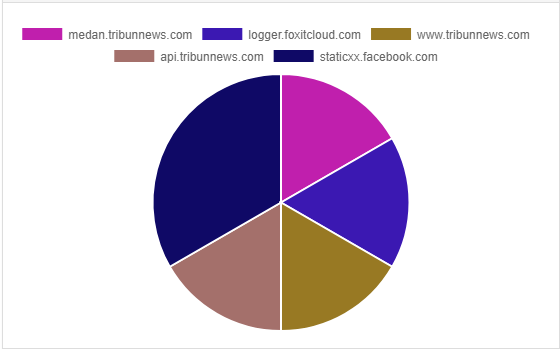
**2017**

**ANALISIS DAN HASIL**

1. **Web Page**

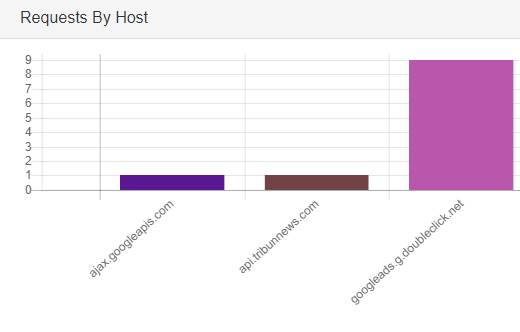
Pada web page (tribunnews.com) destination IP yang paling banyak dituju adalah 172.217.27.98, destination port yang paling banyak dituju adalah 80. Untuk source port nya sendiri paling tinggi berada di 3 yaitu 50533. Pada konektifitas oleh protokolnya sendiri paling banyak menggunakan protocol UDP daripada TCP.

Jika dilihat dari analisis DNS nya, permintaan yang paling banyak terjadi pada tribunnews sendiri lebih banyak dari redirect Facebook. Selama capture data tidak ada error yang terjadi.



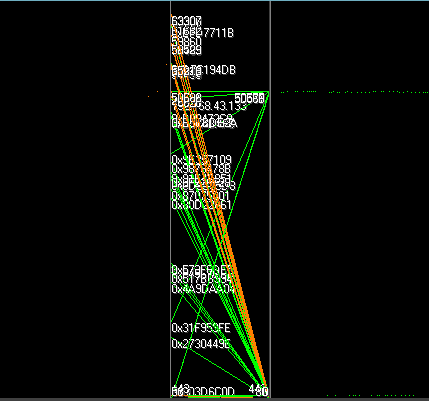
**Gambar 1**. Sumber Request

Google Ads juga paling banyak berpengaruh terhadap web page ini dimana host permintaaan sering diajukan oleh google Ads sendiri dan yang kedua adalah api.tribunnews.com.

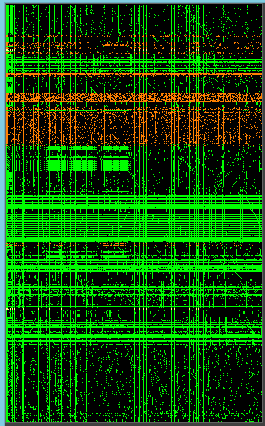


**Gambar 2**. Request By Host.

Selain itu, permintaan destination IP-nya banyak bersumber dari 34.199.213.204 dimana permintaannya sebesar 3 dengan waktu 2 menit. Seluruh destination port yang digunakan adalah 443. Server tribunnews sendiri paling besar pada logger.foxitcloud.com, facebook.com, s0.2mdn.net dan google.com. Meskipun sumber server ada beberapa dari HTTP namun untuk tribunnews sendiri paling banyak menggunakan SSL.



**Gambar 3.** Web Page UDP Source

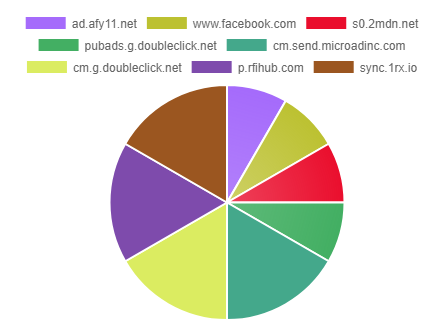


**Gambar 4.** Bit Frekuensi Paket Data Web Page

1. **Video Streaming**

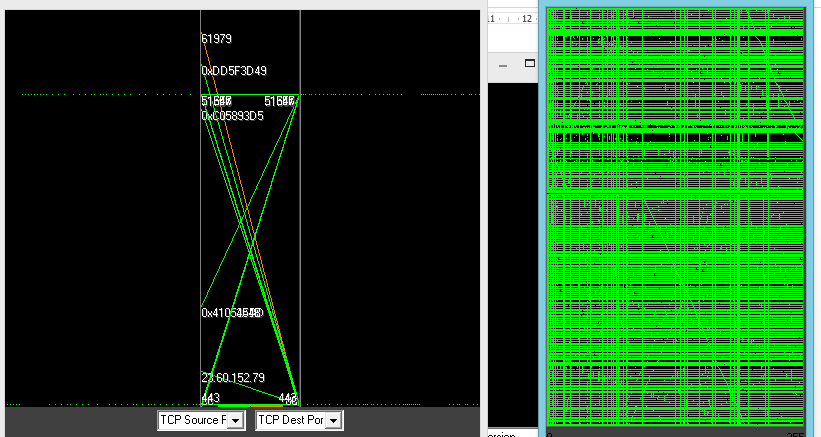
Link yang digunakan pada percobaan ini adalah video.com dimana penulis mengakses salah satu video berdurasi 2:08 dan hanya di capture data selama 2 menit. Pada link ini protocol yang paling banyak digunakan adalah TCP dimana servicenya sendiri banyak berasal dari HTTP. Konektivitas destination portnya juga banyak terjadi pada 443 dimana skalanya lebih dari 50. Destination IP yang banyak digunakan adalah 172.217.27.34.

Permintaan yang banyak terjadi pada video.com ini paling besar berasal dari sync.1rx.io, cm.g.doubleclick.net dan ad.afy11.net.



**Gambar 5.** Sumber Permintaan dari link video.com.

Response codenya terjadi buffering dimana 30 persennya adalah unknown. Permintaan yang paling banyak dari destination IP adalah 210.160.193.173 dan destination port 443.



**Gambar 6.** Hasil Visualisasi PCAP Vidio.com

**DAFTAR PUSTAKA**

Anonim. Security Site. <http://asecuritysite.com/forensics/pcap>

Sam Class. Project 3: Analyze Packet Capture File. <https://samsclass.info/106/proj13/p3_Wireshark_pcap_file.htm>

Reeves, Scott. 2012. Two Simple Filters for Wireshark to Analyze TCP and UDP Traffic. <http://www.techrepublic.com/blog/linux-and-open-source/two-simple-filters-for-wireshark-to-analyze-tcp-and-udp-traffic/>