Tugas Manajemen Keamanan Informasi
“Analisis War Driving Menggunkan Tools Wigle dan Mapping menggunakan Google Earth Dikawasan KM 32 Indralaya”

Dahlia 09031181520117

Jurusan Sitem Informasi
Fakultas Ilmu Komputer
Universitas Sriwijaya
2018

Pendahuluan

War Driving merupakan proses mengumpulkan informasi mengenai jarinngan wireless pada suatu kawasan dengan cara berkiliking kawasan tersebut yang bisa terjangkau sinyal dari jaringan wireless tersebut.

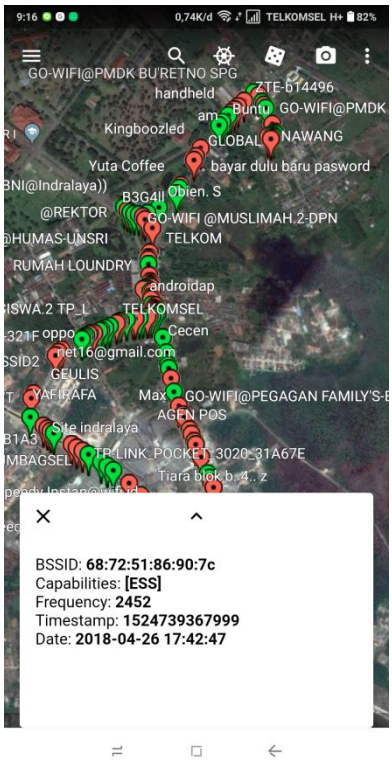
Tools yang digunakan yaitu Wigle Wifi dan Google Earth. Wigle WiFi digunakan untuk scanning jaringan wireless yang berada disekitar lokasi kita berdasarkan GPS pada smartphone. Aplikasi wigle aan mengeluarkan output dari hasil scanning dalam bentuk CSV tau KML. Kali ini kita akan menggunakan bentuk KML untuk menyimpan hasil scanning pada database. Kemudian dapat dipetakan menggunakan aplikasi Google Earth dengan membuka file KML yang tersimpan.

Berikut ini merupakan hasil dari war driving yang telah dilakukan pada daerah sekitar Kos HMS Indralaya – Timbangan KM 32 – Kos HMS Indralaya.

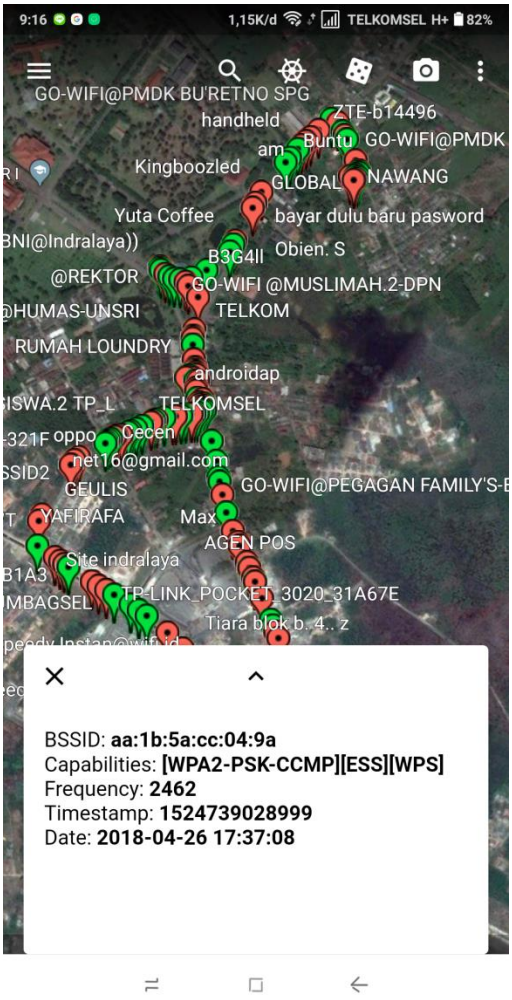
Gambar diatas merupakan hasil dari war driving dengan scanning menggunakan Wigle yang dipetakan menggunakan Google Earth.

Pada hasil mapping diatas, terdapat beberapa access point di kawasan tersebut. Pada gambar diatas terdapat titik-titik yang bewarna hijau dan merah yang merupakan titik access point yang didapat dari hasil scanning.

- Titik access point yang berwarna hijau menyatakan bahwa *Access Point (AP)* tersebut menggunkan metode autentikasi dengan *service* radius. Jaringan wireless yang bewarna hijau ini memiliki akses yang bisa di buka siapa saja tetapi dibatasi dengan jarak radius yang dapat dijangkau.
- Titik access point yang bewarna merah menyatakan bahwa *Access Point (AP)* tersebut dilindungin oleh *passwo\rd* dengan metode autentikasi WE/WPA-PSK/WPA2-PASK. Jaringan wireless yang bewarna merah ini memiliki akses tertutup yang berarti hanya orang yang mengetahui password yang bisa menggunakan jaringan wireless tersebut.



Salah satu SSID yang ditemukan yaitu “Max”. SSID “Max” ini memiliki:
BSSID = 68:72:51:86:90:7c yaitu jenis enkripsi yang digunakan pada wifi tersebut .
Capabilities = [ESS] yaitu kemanan yang digunakan oleh SSID tersebut. ESS (Extended Service Set) berarti menggunakan lebih dari satu Access point atau lebih dari satu BSS (satu access point kejaringan internet) dalam satu jaringan
Frequency = 2452 yaitu frekuensi kekuatan sinyal yang dimiliki.
Timestamp = 1524739367999
Date = 2018-04-26 17:42:47 merupakan waktu kapan jaringan wireless ini tertangkap saat scanning.



BSSID = aa:1b:5a:cc:04:9a yaitu jenis enkripsi yang digunakan pada wifi tersebut .
Capabilities = [WPA2-PSK-CCMP][ESS][WPS] yaitu kemanan yang digunakan oleh SSID tersebut. WPA2 adalah sertifikasi produk yang tersedia melalui Wi-Fi Alliance. WPA2 Sertifikasi hanya menyatakan bahwa peralatan nirkabel yang kompatibel dengan standar IEEE 802.11i. WPA2 sertifikasi produk yang secara resmi menggantikan wired equivalent privacy (WEP) dan fitur keamanan lain yang asli standar IEEE 802.11. WPA2 tujuan dari sertifikasi adalah untuk mendukung wajib tambahan fitur keamanan standar IEEE 802.11i yang tidak sudah termasuk untuk produk-produk yang mendukung WPA.
Frequency = 2426 yaitu frekuensi kekuatan sinyal yang dimiliki.
Timestamp = 1524739028999
Date = 2018-04-26 17:37:08 merupakan waktu kapan jaringan wireless ini tertangkap saat scanning.