Laporan Manajemen Keamanan Informasi
“Wardriving”

Erdo Irawan 09031281520097

Jurusan Sitem Informasi
Fakultas Ilmu Komputer
Universitas Sriwijaya
2018

- ✓ Wardriving

  Wardriving adalah tindakan mencari jaringan nirkabel Wi-Fi dengan seseorang dalam kendaraan yang bergerak, menggunakan komputer portabel, smartphone atau personal digital assistant (PDA). Seseorang berkeliling ke berbagai tempat dalam usahanya mencari, mengexplorasi, bahkan mungkin juga mengeksploitasi jaringan wireless yang ditemukannya. Kemudian orang yang melakukan kegiatan tersebut disebut sebagai "Wardriver", dalam upayanya itu dia melakukan pengumpulan data, membuat pemetaan area-area yang ada jaringan wirelessnya, dan menganalisa sistem securitynya. Kata Wardriving ini ada kaitannya bahwa sang wardriver menggunakan kendaraan bermotor untuk beraktivitas berkeliling ke berbagai tempat. Tujuannya berbagai macam mulai dari hanya sekedar ingin tahu, melakukan riset, hobi, menyadap untuk mendapatkan informasi rahasia, bahkan ada yang bertujuan untuk meyakinkan para pengguna dan pabrikan perangkat wireless untuk memperbaiki sistem keamanan mereka.

- ✓ Wigle

  Wigle adalah salah satu aplikasi yang tersedia untuk perangkat android pada smartphone yang digunakan untuk melakukan wardriving dengan perangkat mobile android. Tools ini sudah terhubung dengan GPS yang ada pada smartphone dan dengan file yang sudah kita save pada smartphone kita, kita dapat memetakannya pada map yang tersedia dengan mengekport file mapping wardriving yang ada pada smartphone. Aplikasi Wigle ini dapat mengeluarkan output dari hasil scanning kedalam bentuk csv ataupun Kml untuk menyimpan database yang digunakan oleh data terdapat pada aplikasi tersebut yang akan digunakan ketika kita ingin melakukan mapping hotspot wi-fi.

- ✓ Wireless Access Point

  Wireless Access Point (WAP) dalam jaringan komputer , titik akses nirkabel adalah suatu peranti yang memungkinkan peranti nirkabel untuk terhubung ke dalam jaringan dengan menggunakan Wi-Fi, Bluetooth, atau standar lain. WAP biasanya tersambung ke suatu *router* (melalui kabel) sehingga dapat meneruskan data antara berbagai peranti nirkabel (seperti komputer atau pencetak) dengan jaringan berkabel pada suatu jaringan. Standar yang diterapkan untuk WAP ditetapkan oleh IEEE dan sebagian besar menggunakan IEEE 802.11. WAP terhubung pada jaringan, pada jarak jangkauan WAP siapapun dapat terhubung ke jaringan . Pada saat ini enkripsi merupakan keamanan standar yang harus dimiliki oleh setiap Access Point yang digunakan sebagai sistem keamanan yang kaan menjamin keamanan user. Generasi enkrispi pertama yang diterapkan adalah Wired Equivalent Privacy (WEP), WEP sendiri telah banyak diuji karna memeliki banyak kelemaha sehingga sangat mudah untuk ditembus. generasi kedua dan ketiga adalah menggunakan Wi-Fi Protected Access (WPA), Beberapa WAP mendukung authentication menggunakan Remote Authentication Dial-In User Service (RADIUS) dan server authentication yang lain . dan digenerasi yang sama Wi-Fi Protected Access II (WPA2), keduanya memiliki algoritma yang kuat dan aman jika menggunakan password atau passphrase yang kuat (unik).

- ✓ GPS

  Global Position System (GPS) adalah sistem untuk menentukan letak di permukaan bumi dengan bantuan penyelarasan (*synchronization*) sinyal satelit. Sistem ini menggunakan 24 satelit yang mengirimkan sinyal gelombang mikro ke Bumi. Sinyal ini diterima oleh alat penerima di permukaan, dan digunakan untuk menentukan letak, kecepatan, arah, dan waktu.

- ✓ Google Earth

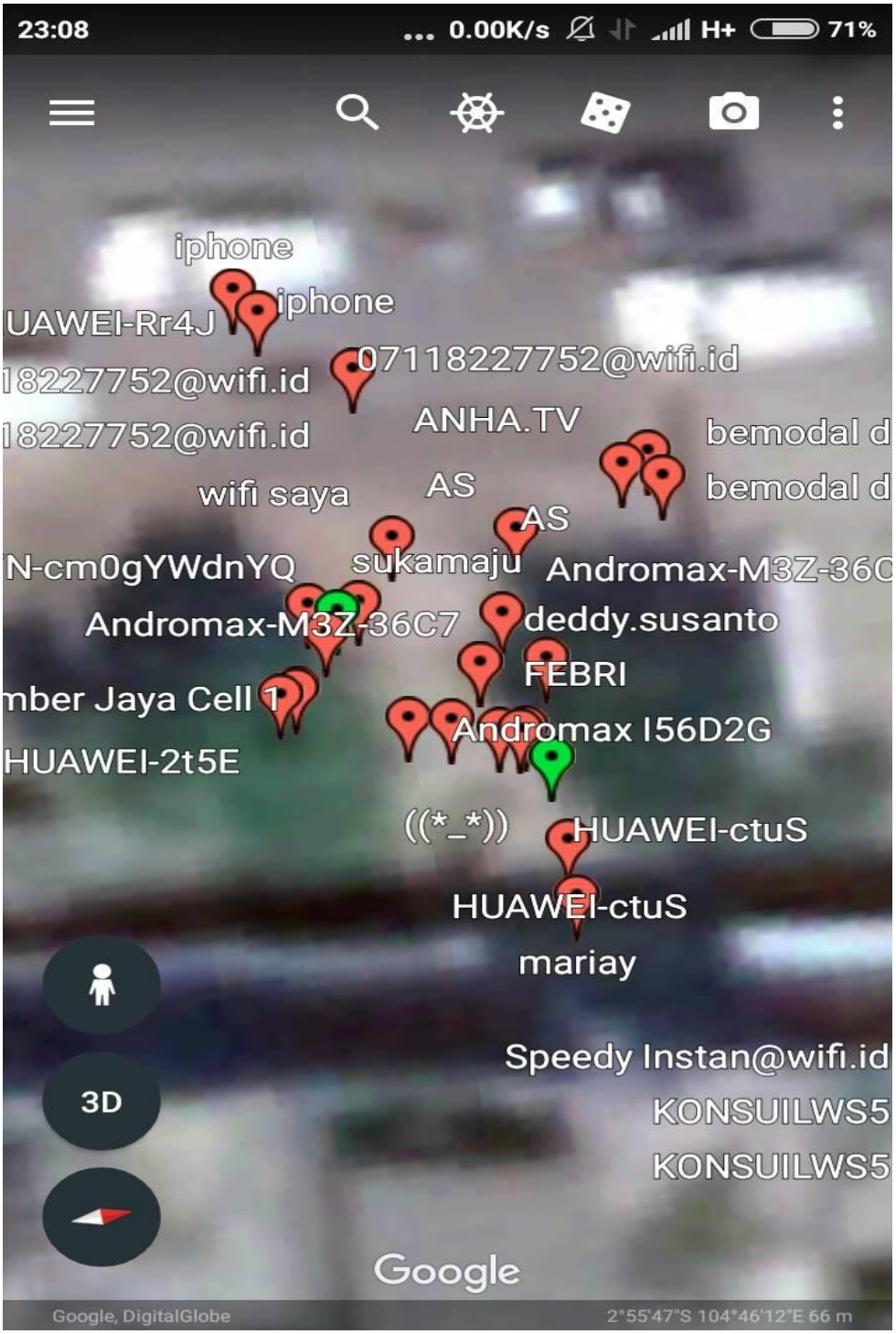
  Google Earth merupakan sebuah program globe virtual yang sebenarnya disebut Earth Viewer dan dibuat oleh Keyhole, Inc.. Program ini memetakan bumi dari superimposisi gambar yang dikumpulkan dari pemetaan satelit, fotografi udara dan globe GIS 3D.

Dalam melakukan wardriving ini, tools yang digunakan adalah :
1.Smartphone dengan sistem operasi Android.
2. Wardriving Tools : WiGle Wifi
3. Mapping Wi-fi Tools : Google Earth

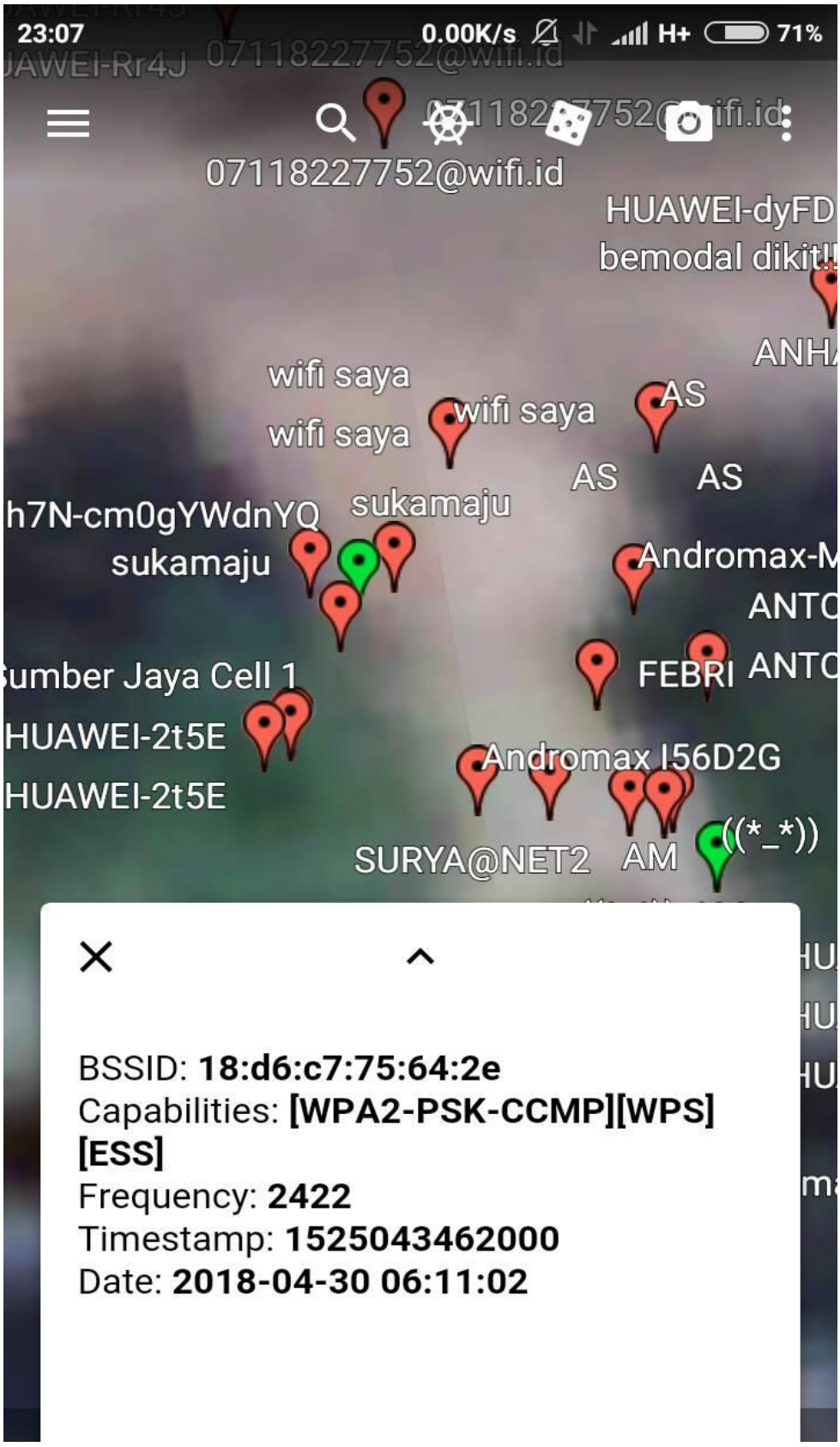
Pada percobaan kali ini, yang menjadi target adalah area jalanan disekitar Palembang. Tindakan wardriving menggunakan kendaraan sepeda motor untuk berkeliling di sekitar jalanan, setelah itu mulai menghidupkan GPS pada smartphone android dan membuka aplikasi WiGle wifi. Dalam perjalanan aplikasi pada smartphone telah mulai melakukan scanning wireless network dan setelah beberapa saat sudah terlihat kumpulan wireless network muncul pada layar smartphone, kemudian setelah mendapatkan kumpulan wireless network yang diinginkan, maka database dieksport dalam bentuk file dengan format .kml dimana file ini akan diimport kedalam aplikasi mapping tools google earth yang sudah terinstall di smartphone sebelumnya untuk mendapatkan hasil mapping berupa lokasi wireless network yang ada.

✓ Hasil dan Analisa

Hasil dari proses mapping wireless network dengan menggunakan aplikasi google earth adalah sebagai berikut :



Gambar 1


23:07
0.00K/s
H+
71%
07118227752@wifi.id
HUAWEI-dyFD
bemodal dikit!!
wifi saya
wifi saya
wifi saya
AS
AS
AS
sukamaju
sukamaju
Andromax-M
FEBRI
HUAWEI-2t5E
HUAWEI-2t5E
Andromax I56D2G
SURYA@NET2
AM
((*_*))
BSSID: 18:d6:c7:75:64:2e
Capabilities: [WPA2-PSK-CCMP][WPS][ESS]
Frequency: 2422
Timestamp: 1525043462000
Date: 2018-04-30 06:11:02

Gambar 2

Setelah melakukan scanning didapatlah file format .kml yang diexport dari Wigle,dan langsung dibuka file tersebut dengan menggunakan GoogleEarth, hasil yang didapat dari Google Earth adalah mapping yang bisa dilihat pada Gambar 1 , dapat dilihat pada mapping bahwasannya hasil scanning juga mengenai beberapa Access Point milik beberapa Provider terkenal yang ada di Indonesia yang juga memiliki Hotspot dikawasan tersebut yaitu wifi.id yang merupakan wireless network berbayar milik perusahaan TELKOMSEL . Pada gambar 1 terlihat ada ikon berwarna merah dan hijau, ikon berwarna merah menyatakan bahwa Access Point (AP) tersebut dilindungi oleh password dengan metode autentikasi WEP/WPA PSK/WPA2-PSK, sementara ikon yang berwarna hijau menyatakan bahwa Access Point (AP) tersebut menggunakan metode autentikasi dengan servis RADIUS.

Pada gambar 2, kita tentukan wi-fi yang akan dijadikan sampel untuk mendapatkan informasi tentang access point dari wireless network tersebut, pada gambar didapatkan informasi bahwa wireless network sukamaju memiliki BSSID yaitu 18:d6:c7:75:64:2e, frekuensi sinyal yang dimiliki adalah 2422, kapabilitas yang dimiliki network tersebut adalah [WPA PSK-CCMP][WPS][ESS] dimana CCMP singkatan Kontra mode CBC-MAC Protocol. CCMP, juga dikenal sebagai AES CCMP, adalah mekanisme enkripsi yang telah menggantikan TKIP, dan itu adalah standar keamanan yang digunakan dengan jaringan nirkabel WPA2. Menurut spesifikasi, jaringan WPA2 harus menggunakan CCMP secara default (WPA2-CCMP), meskipun CCMP juga dapat digunakan pada jaringan WPA untuk meningkatkan keamanan (WPA-CCMP).

- ✓ Kesimpulan

  Dari proses wardriving yang dilakukan di atas, dapat ditarik kesimpulan :

  a. GoogleEarth bisa digunakan untuk mapping sebuah jaringan wireless sebagai pendukung kegiatan Wardriving, dan juga dapat mengetahui SSID serta BSSID yang ada pada jaringan wireless tersebut ,tentu saja mapping bisa dilakukan dengan format file .kml yang diberikan oleh Wigle.
  b. Kekuatan sinyal dari suatu access point bergantung pada jarak (range), semakin jauh area cakupan lokasi akses dari suatu access point, maka semakin lemah sinyal yang diterima oleh pengguna access point tersebut dan sebaliknya.
  c. Semakin luas daerah yang menjadi target untuk proses wardriving, maka semakin banyak potensial ditemukan access point yang menjadi sumber wi-fi.
  d. Access point yang memiliki proteksi pada jaringannnya, misalnya access point yang dilindungi oleh password SSID(WPA2 – PSK atau WPA PSK) masih rentan (vulnerable) dari ancaman dari pihak asing (attacker) dari ancaman attacker, apalagi access point yang tidak memiliki sistem proteksi pada jaringannya sama sekali.