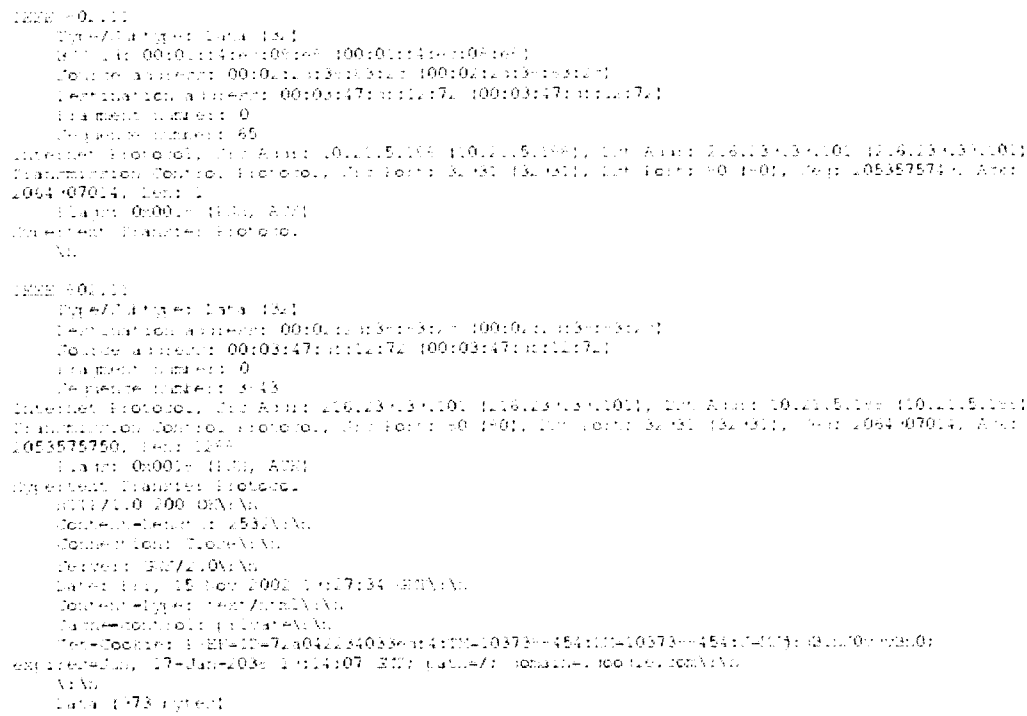
Dalam data diatas kita dapat melihat pertukaran data TCP diantara eve dan vic, dengan informasi ini kita dapat memulai bahwa 802.11 digunakan oleh masing-masing klien, mengidentifikasi vic menggunakan perurutan dalam range 2378-2380 dimana eve menggunakan nomorm perurutan dalam range 57-58.
Dalam trace dibawah ini kita mengetahui bahwa membuat koneksi ke google.com dengan pertukaran NetBios.

```
IEEE 802.11
    Type/Subtype: Data (32)
    Source address: 00:02:[illegible] (00:02:[illegible])
    Destination address: 00:03:47:[illegible]:72 (00:03:47:[illegible]:72)
    Fragment number: 0
    Sequence number: 62
Internet Protocol, Src Addr: 10.21.5.[illegible] (10.21.5.[illegible]), Dst Addr: 216.23[illegible].3[illegible].101 (216.23[illegible].3[illegible].101)
Transmission Control Protocol, Src Port: 32[illegible]31 (32[illegible]31), Dst Port: 80 (80), Seq: [illegible]053575733, Ack: 0, Len: 0
    Flags: 0x0002 (SYN)

IEEE 802.11
    Type/Subtype: Data (32)
    Destination address: 00:02:[illegible] (00:02:[illegible])
    Source address: 00:03:47:[illegible]:72 (00:03:47:[illegible]:72)
    Fragment number: 0
    Sequence number: 3[illegible]41
Internet Protocol, Src Addr: 216.23[illegible].3[illegible].101 (216.23[illegible].3[illegible].101), Dst Addr: 10.21.5.[illegible] (10.21.5.[illegible])
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 32[illegible]31 (32[illegible]31), Seq: [illegible]064[illegible]07013, Ack: [illegible]053575734, Len: 0
    Flags: 0x0012 (SYN, ACK)

IEEE 802.11
    Type/Subtype: Data (32)
    Source address: 00:02:[illegible] (00:02:[illegible])
    Destination address: 00:03:47:[illegible]:72 (00:03:47:[illegible]:72)
    Fragment number: 0
    Sequence number: 63
Internet Protocol, Src Addr: 10.21.5.[illegible] (10.21.5.[illegible]), Dst Addr: [illegible]16.23[illegible].3[illegible].101 (216.23[illegible].3[illegible].101)
Transmission Control Protocol, Src Port: 32[illegible]31 (32[illegible]31), Dst Port: 80 (80), Seq: [illegible]053575734, Ack: 2064[illegible]07014, Len: 0


    Flags: 0x0010 (ACK)

IEEE 802.11
    Type/Subtype: Data (32)
    Source address: 00:02:[illegible] (00:02:[illegible])
    Destination address: 00:03:47:[illegible]:72 (00:03:47:[illegible]:72)
    Fragment number: 0
    Sequence number: 64
Internet Protocol, Src Addr: 10.21.5.[illegible] (10.21.5.[illegible]), Dst Addr: 216.23[illegible].3[illegible].101 ([illegible].23[illegible].3[illegible].101)
Transmission Control Protocol, Src Port: 32[illegible]31 (32[illegible]31), Dst Port: 80 (80), Seq: [illegible]053575734, Ack: 2064[illegible]07014, Len: 15
    Flags: 0x001[illegible] ([illegible], ACK)
Hypertext Transfer Protocol
    GET / HTTP/1.0\n

IEEE 802.11
    Type/Subtype: Data (32)
    Destination address: 00:02:[illegible] (00:02:[illegible])
    Source address: 00:03:47:[illegible]:72 (00:03:47:[illegible]:72)
    Fragment number: 0
    Sequence number: 3[illegible]42
Internet Protocol, Src Addr: 216.23[illegible].3[illegible].101 (216.23[illegible].3[illegible].101), Dst Addr: 10.21.5.[illegible] (10.21.5.[illegible])
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 32[illegible]31 (32[illegible]31), Seq: 2064[illegible]07014, Ack: [illegible]05357574[illegible], Len: 0
    Flags: 0x0010 (ACK)
```



Gambar 12 Trace Koneksi

Setelah menganalisa dengan lebih dekat, kita melihat bahwa MAC ADDRESS vic (00:02:2d:38:83:2c) adalah bukan dengan memakai perurutan previously established baseline. Agaknya, pengurutan nomor ideal yang lebih dekat merefleksikan eve dalam range 62-65, dengan informasi seperti ini dapat pula kita simpulkan **bahwa MAC ADDRESS 00:02:2d:38:83:2c telah diperdayai dengan Mac spoofing oleh 00:02:2d:09:a1:dd (Eve).**

7. Penutup

Teknik kejahatan carding adalah salah satu dari sekian banyak varian kejahatan komputer, efek yang ditimbulkan biasanya lebih bersifat ke ekonomi. Tindakan yang dilakukan secara preventif kepada keamanan sistem komputer adalah lebih baik untuk dilakukan, selain itu juga konsumen kartu kredit hendaknya selalu waspada terhadap informasi-informasi yang tidak jelas sumbernya, yang biasanya sering digunakan carder untuk mengecoh korbannya.

Handalnya sistem keamanan jaringan tanpa kabel bukan berarti membuat 100% jaringan akan bebas dari masalah keamanan, perlu intensifitas, kejelian untuk membuat sistem jaringan aman, minimalnya memperkecil potensi rusaknya keamanan. Kewaspadaan seorang admin jaringan memang sangat perlukan, selain itu hendaknya selalu menambah dengan wawasan-wawasan baru mengenai topik sekuritas, karena akan selalu berkembang dari waktu ke waktu. Penyebaran tool-tool keamanan yang tersedia gratis di internet akan tergantung proposi penggunaannya oleh si pemakai, untuk tujuan positif ataupun negatif[5].

Dalam informasi tersebut, pentingnya keamanan jaringan komputer tanpa kabel seakan-akan menjadi kebutuhan vital yang level kepentingan nya sama dengan tujuan penggunaannya. Disatu sisi semakin tingginya kebutuhan manusia akan teknologi seakan-akan membuat kebutuhan akan teknologi menjadi kebutuhan primer yang akan dengan mudahnya menghalalkan segala cara.

Kami berharap laporan ini nantinya akan menjadi referensi yang berharga untuk peminat investigasi forensik cybercrime khususnya, serta pecinta Teknologi Informasi pada umumnya. *Wallahu A'lam*.

[5] Anonim, "*Computer Hacking Forensics Investigator*", *Module 7 WINDOWS FORENSICS* EC-Council, 2006

Glossary

- Registry : Keterangan dasar berkaitan dengan mesin komputer (hardware dan software)
- Inurl : perintah untuk melakukan pencarian carding di search engine
- Proxy : fasilitas untuk menghubungkan diri ke internet secara bersama-sama/sharing
- Ip address : pengalamatan komputer yang terseting dalam internet
- Courier service : jasa pengantar barang
- MAC address :Nomor unik hardware oleh pabrik
- MAC Spoofing dan filtering :Aktivitas Pencurian MAC ADDRESS dan pemakaian
- Investigator :Pengusut kasus
- IEEE : Asosiasi internasional yang membuat standar pengalamatan ip
- APJII :Asosiasi penyedia Nomor Publik untuk internet di indonesia
- Bluetooth :Teknologi tanpa kabel standar 802.15.1
- Local Area Networking:Jaringan Komputer dalam ruangan yang sama
- Acces Point (AP) :perangkat hardware untuk koneksi jaringan wireless
- SSID :nama workgroup dalam jaringan wireless
- fungsi ioctl() : Program berbahasa C untuk mengganti MAC ADDRESS
- Brute force :Serangan terus menerus dengan mencoba list phrase satu persatu
- NetFlow :aplikasi untuk men-undeteksi komputer di jaringan
- passive monitoring :Pemantauan traffic secara pasif
- Three-byte :tiga digit pertama MAC ADDRESS
- Tcpdump :aplikasi untuk mengcapture kondisi jaringan
- Denial of Service (DoS) :Serangan bertubi-tubi pada komputer(service) untuk meminta service/respon
- blue screen of death :tampilan biru pada monitor yang menandakan komputer hang
- Enkripsi :metode pengamanan dengan teknik agar tidak terbaca oleh yang tak berhak
- Default gateway :perantara dalam jaringan yang berperan sebagai penghubung yang terseting secara default (natural)
- Network Intrusion Detection System-NIDS :sistem pendeteksi bilamana terjadi indikasi gangguan pada jaringan

Daftar Pustaka

[JHO06] Jhonsen, Jhon Edison, *"Membangun Wireless LAN"*, Jakarta : Penerbit PT Elex Media Komputindo Kelompok Gramedia Jakarta, Januari 2006

[PCP06] PC PLUS (PC+), *"Membangun Wireless LAN mudah dan murah"*, Jakarta : PT Prima Infosarana Media, Desember 2006

[WRI03] Wright, Joshua, *"Detecting Wireless LAN MAC ADDRESS Address Spoofing"*, CCNA, Januari 2003

[ANO06] Anonim, *"Computer Hacking Forensics Investigator", Module 7 WINDOWS FORENSICS* EC-Council, 2006.

[YOG05] Anonim, Situs Komputer, http://www.yogyafree.net/, diakses pada Januari 05