Farid Wazdi
09111001047
Keamanan Jaringan Komputer

1. Gunakan salah satu tools forensic dan beri penjelasan.

Pada tugas kali ini, penulis akan menggunakan salah satu tools forensic free for windows yang bernama “Network Miner”. Apa itu Network Miner? Network Miner adalah alat analisis forensik jaringan (NFAT) untuk Windows. NetworkMiner dapat digunakan sebagai alat pengintai paket jaringan pasif yang dapat digunakan untuk mendeteksi sistem operasi, sesi, nama host, open port dll tanpa perlu menempatkan lalu lintas di jaringan secara langsung. NetworkMiner juga dapat menguraikan file PCAP untuk analisis off-line dan meregenerasi / menyusun kembali file yang dikirim dan sertifikat dari file PCAP.

Tujuan NetworkMiner adalah untuk mengumpulkan data (seperti bukti forensik) tentang host di jaringan, daripada mengumpulkan data mengenai lalu lintas jaringan. Tampilan utama adalah host centric (informasi dikelompokkan per host) daripada packet centric (informasi ditampilkan sebagai daftar paket / frame).

NetworkMiner melakukan OS fingerprinting berdasarkan TCP SYN dan SYN + ACK paket dengan menggunakan database OS fingerprinting dari p0f dan Ettercap. NetworkMiner juga dapat melakukan fingerprinting OS berdasarkan paket DHCP dengan memanfaatkan Satori OS fingerprinting database dari FingerBank. NetworkMiner juga menggunakan daftar vendor-MAC dari Nmap.

NetworkMiner dapat mengekstrak file dan sertifikat yang ditransfer melalui jaringan dengan memparsing file PCAP atau dengan menyadap lalu lintas langsung dari jaringan. Ini adalah salah satu fungsi yang apik yang dapat digunakan untuk mengekstrak dan menyimpan file media (seperti file audio atau video) yang dialirkan melalui jaringan. Protokol yang didukung untuk ekstraksi file adalah FTP, HTTP dan SMB.

Farid Wazdi
09111001047
Keamanan Jaringan Komputer

Kredensial pengguna (nama pengguna dan kata sandi) untuk protokol yang didukung diekstrak oleh NetworkMiner dan ditampilkan di bawah tab "Kredensial". Maka dari pada itu, harap memperhatikan saat menampilkan konten dari tab ini ke publik.

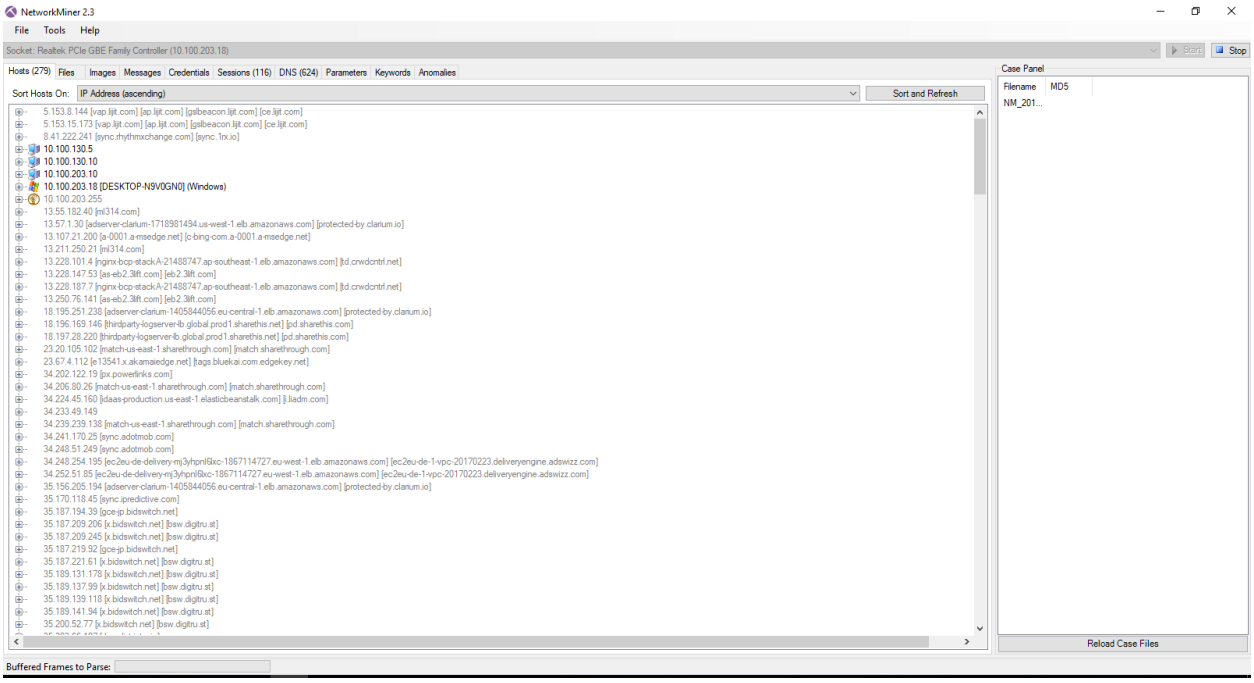
Fitur lain yang sangat berguna adalah bahwa pengguna dapat mencari data yang disadap atau disimpan untuk kata kunci. NetworkMiner memungkinkan pengguna untuk memasukkan string arbitrary atau pola byte yang harus dicari dengan fungsi pencarian kata kunci.

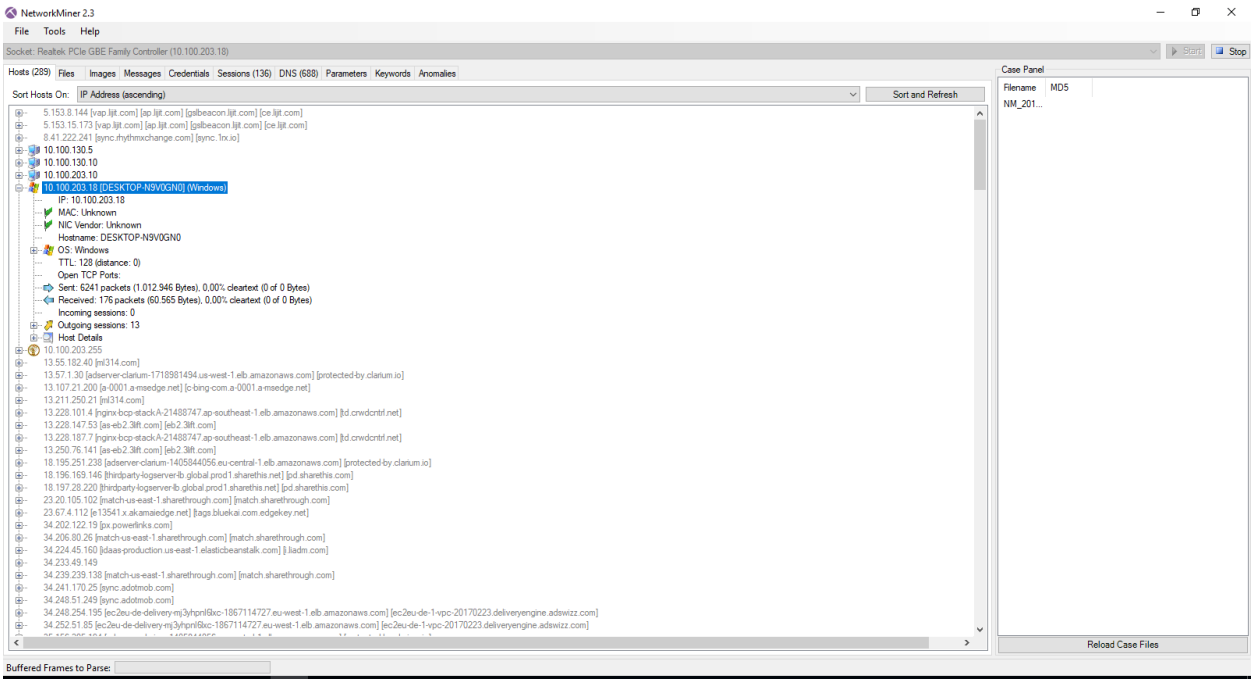
Versi 0.84 (dan yang lebih baru) NetworkMiner telah support atau dapat digunakan untuk menyadap dan mengurai lalu lintas WLAN (IEEE 802.11). NetworkMiner saat ini hanya mendukung WiFi sniffing dengan adaptor AirPcap. Ada juga versi komersial yang tersedia dari NetworkMiner dari Netresec. Versi komersial disebut NetworkMiner Professional dan memiliki fitur tambahan seperti :

- Port Independent Protocol Identification (PIPI)
- Mengekspor hasil ke CSV / Excel
- Direktori keluaran file yang dapat dikonfigurasi
- Pelokalan Geo IP
- Dukungan pewarnaan tuan rumah
- Dukungan skrip baris perintah

Beberapa capture dari penggunaan Network Miner pada windows 10 :

Farid Wazdi
09111001047
Keamanan Jaringan Komputer





Farid Wazdi
09111001047
Keamanan Jaringan Komputer