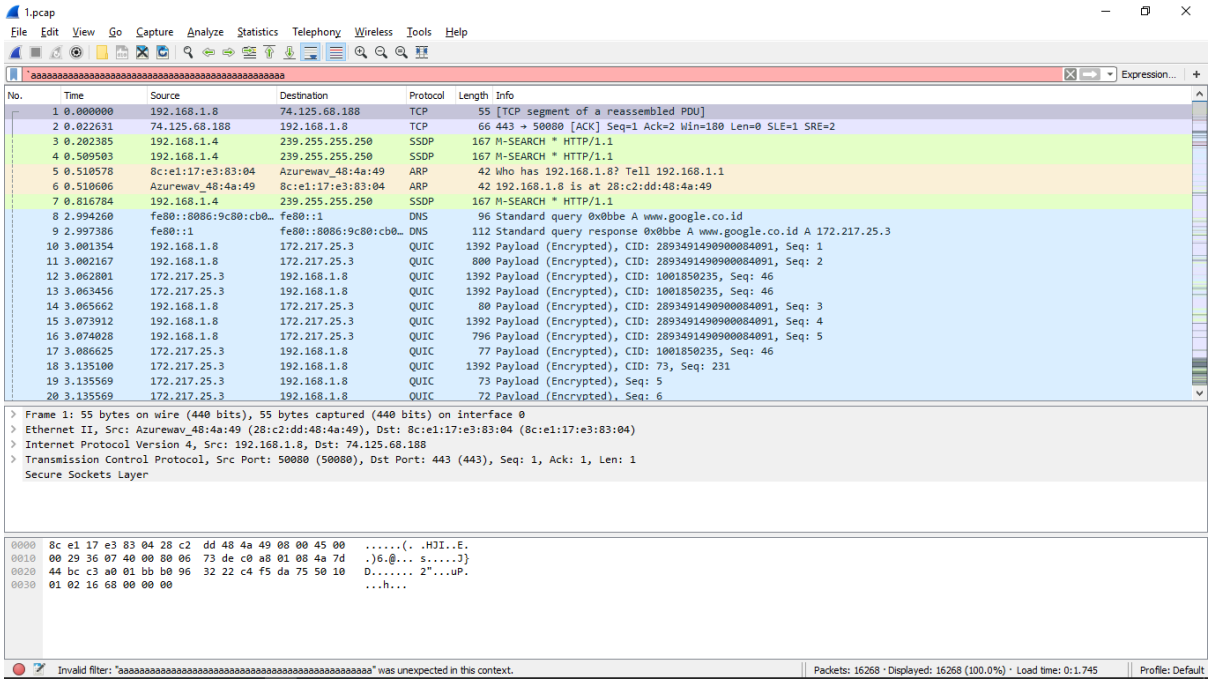
Nama : M. Andre Sofyan

NIM : 09011281520130

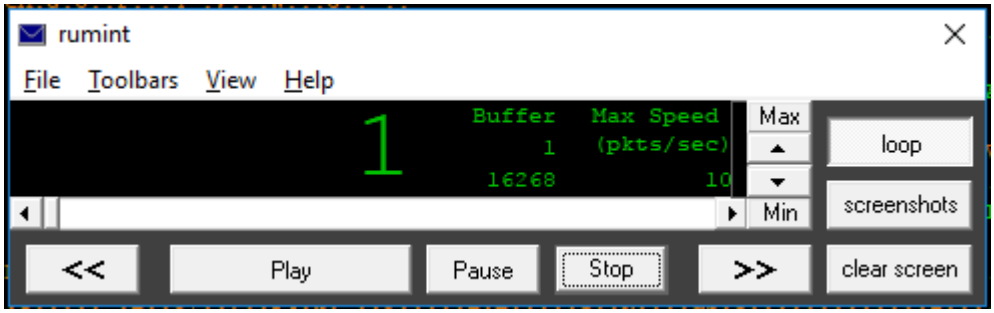
Kelas SK5C

Visualisasi PCAP Data dengan menggunakan Rumint.

Data pcap :



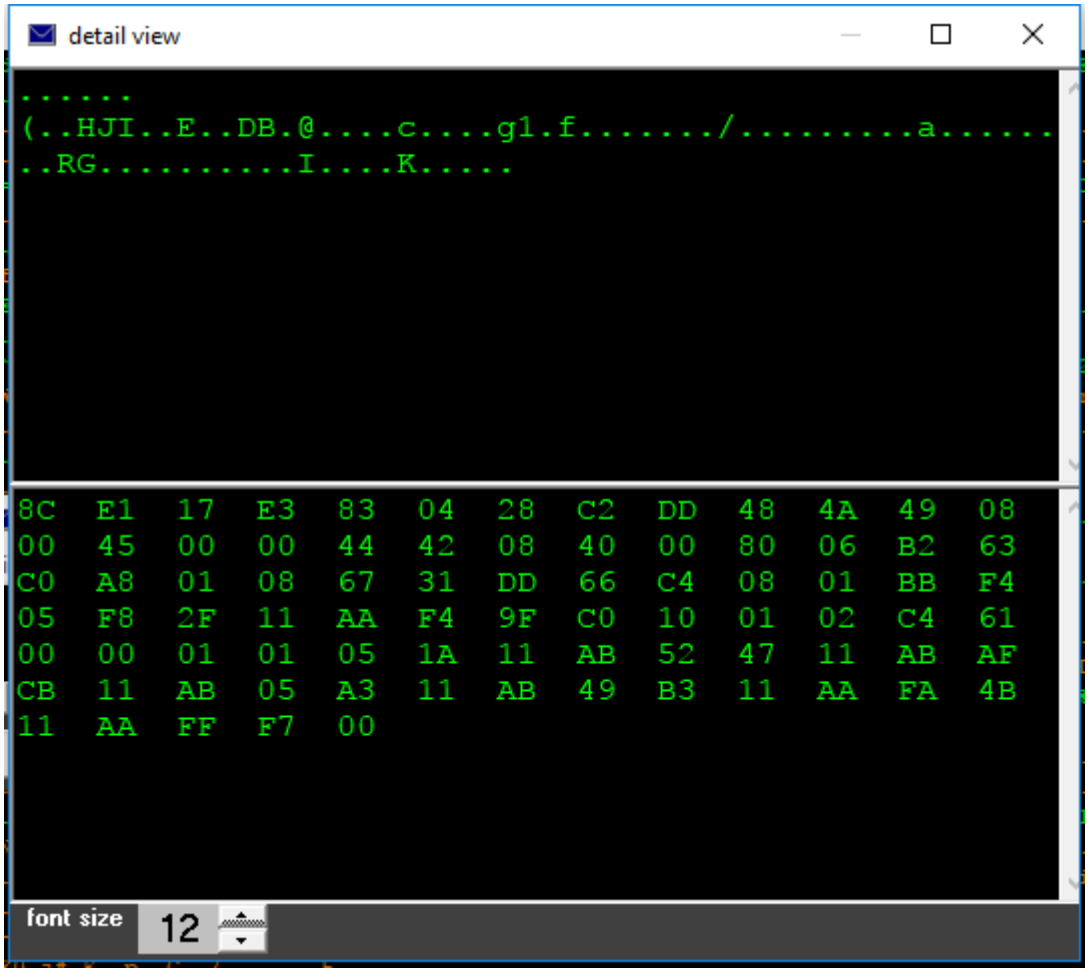
Rumint Tools :



Menafsirkan security visualization images adalah sedikit seperti menafsirkan Rorschach inkblots. Setiap viewer mungkin melihat hal yang berbeda atau tidak sama sekali.

Ping adalah utilitas jaringan yang menguji apakah host dan router dapat dicapai melalui jaringan IP. Ia bekerja dengan mengirimkan Internet Control Message Protocol (ICMP) dengan meminta echo (tipe 0) dan menunggu untuk tujuan untuk menanggapi dengan respon echo ICMP (tipe 8). Jika gagal target merespon dalam waktu yang diberikan waktu ping melaporkan bahwa upaya habis. ICMP echo requests biasanya menggunakan bidang data opsional yang harus mengulang kembali oleh target echo respons tersebut.

Gambar 1 : tradisional paket ICMP dalam ASCII dan heksadesimal.:

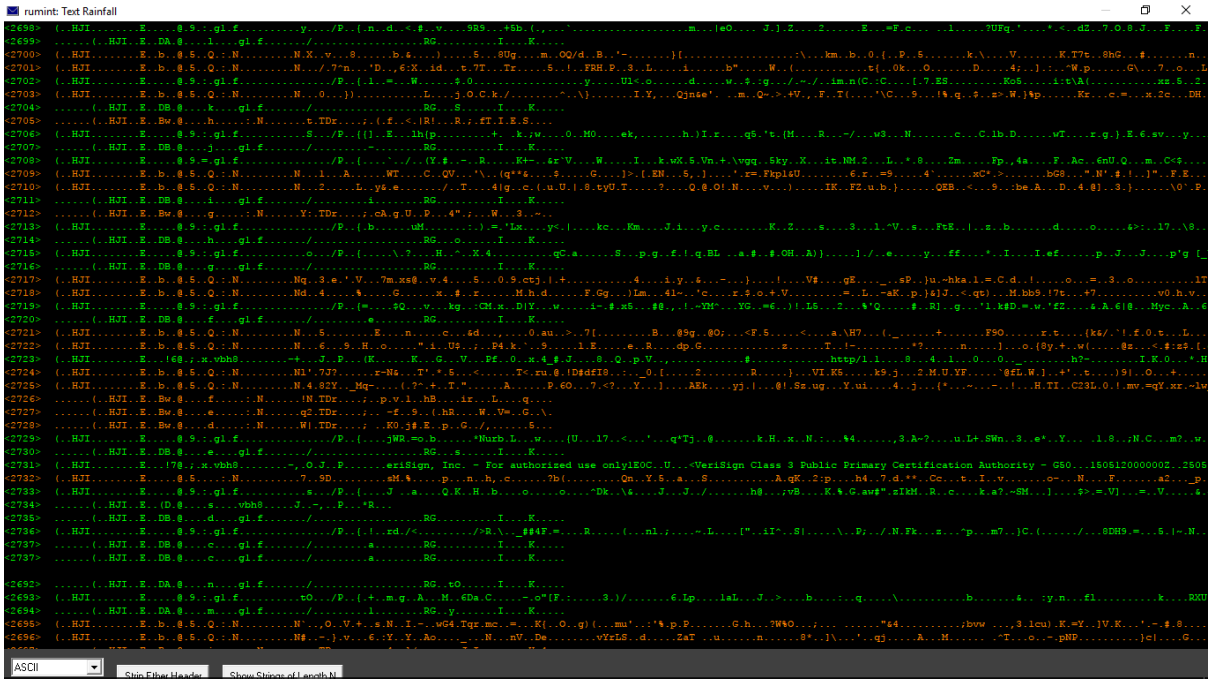


Dengan Capturing the ICMP packets dan menampilkan hasil dalam ASCII seharusnya akan terlihat seperti berikut. Perhatikan bahwa byte tidak di kisaran ASCII dicetak diganti dengan karakter periode.

.....0.....E..<.....$....dBf.....X..N.abcdefghijklmnopqrstuvwabcdefghi
.....0.....E..<.....$....dBf.....X..O.abcdefghijklmnopqrstuvwabcdefghi.
.....0.....E..<.....$....dBf.....X..P.abcdefghijklmnopqrstuvwabcdefghi.
.0.....E..<.....Bf.....d...Y..P.abcdefghijklmnopqrstuvwabcdefghi.
.....0.....E..<.....$....dBf.....X..Q.abcdefghijklmnopqrstuvwabcdefghi.
.0.....E..<.....Bf.....d...Y..Q.abcdefghijklmnopqrstuvwabcdefghi.
.....0.....E..<.....$....dBf.....X..R.abcdefghijklmnopqrstuvwabcdefghi.
.....0.....E..<.....$....dBf.....X..S.abcdefghijklmnopqrstuvwabcdefghi.

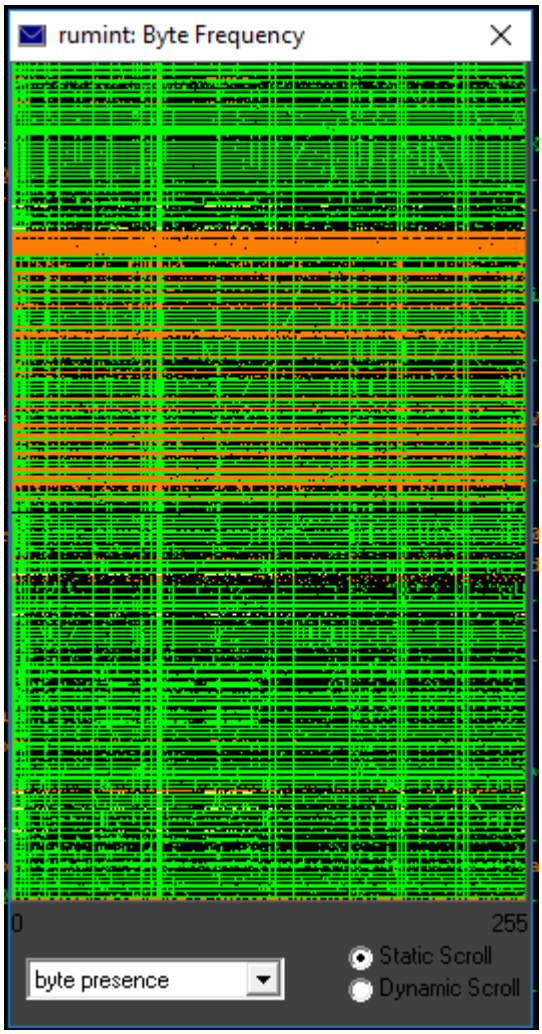
Dari paket ditangkap ini kita melihat bahwa Windows XP menggunakan bagian-bagian dari alfabet huruf kecil untuk bidang data opsional. Kebanyakan Alat yang ada menyediakan teks ASCII dan pemandangan heksadesimal paket dan sistem contoh kami menyediakan fungsi yang sama, seperti yang terlihat dalam gambar diatas.

Gambar 2 : ASCII representasi ICMP jaringan lalu lintas yang dihasilkan oleh perintah ping. Windows XP penggunaan huruf kecil abjad untuk muatan dapat terlihat jelas.



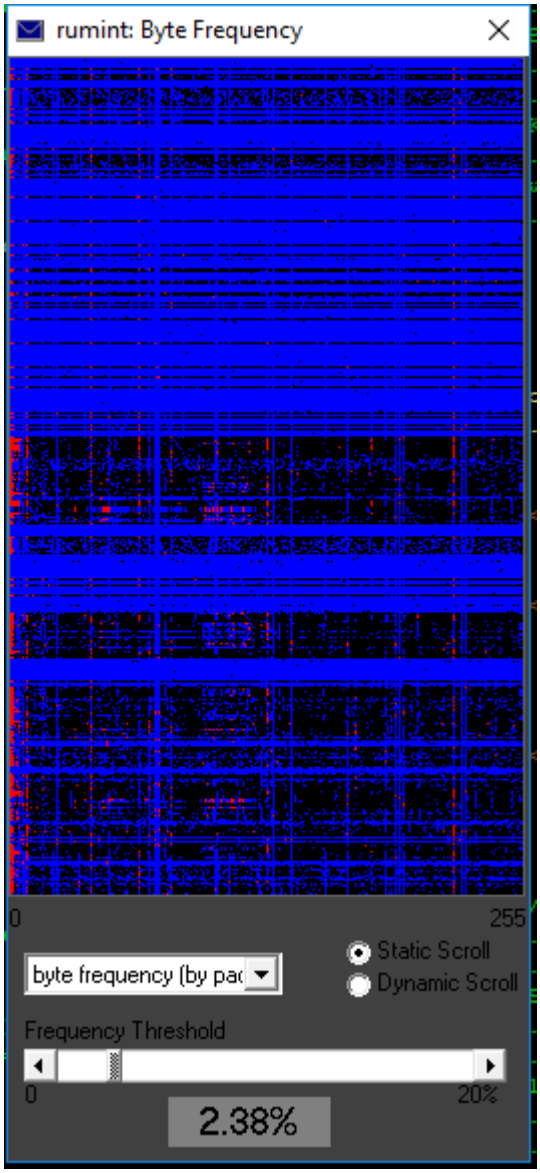
Sedangkan canonical hexadecimal dan pandangan ASCII berguna untuk analisis yang sangat rinci, itu tidak memiliki kemampuan untuk membandingkan angka yang lebih besar dari paket. Untuk tujuan ini, RUMINT menyediakan pandangan curah hujan teks yang memungkinkan 24 sampai 40 paket untuk ditampilkan pada saat yang sama, seperti yang terlihat pada gambar 2. Dari gambar ini kita dapat melihat bahwa banyak paket berperilaku dengan cara yang sama. Sementara ini adalah peningkatan, teks Curah pendapat itu masih terbatas pada sekitar 40 paket pada satu waktu.

Gambar 3: Byte kehadiran perwakilan dari beberapa ratus paket ICMP dihasilkan oleh ping. Paket satu per baris. Bar vertikal yang solid menunjukkan bahwa setiap packet berisi seluruh huruf abjad (ASCII 97-122). Garis diagonal mewakili nilai-nilai secara konsisten berubah antara paket seperti bidang header IP identifikasi.



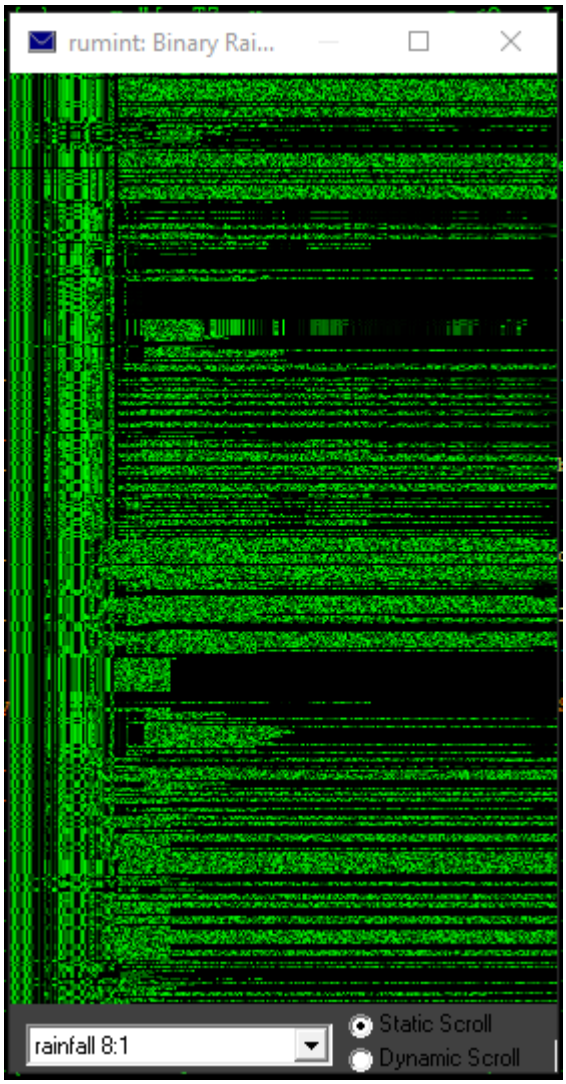
Tampilan kehadiran byte memampatkan informasi ini oleh merencanakan paket satu per baris horisontal. Setiap Jalur horisontal 256 piksel panjang dan piksel sepanjang garis ini menyala didasarkan pada kehadiran byte dalam paket. Sebagai contoh jika paket yang berisi satu byte nilai 97 (ASCII '') kemudian di posisi 97,1 pixel akan diterangi. Jika paket 37 berisi satu byte nilai 122 (ASCII 'z') kemudian di posisi 122,37 pixel akan diterangi. Ketika teknik ini digunakan pada set beberapa ratus paket ICMP hasil dramatis. Gambar 3 memungkinkan kita untuk memastikan bahwa setiap paket muatan kemungkinan dibangun dengan cara yang sama seperti yang ditunjukkan oleh tebal

Gambar 4: Byte frekuensi representasi dari paket-paket yang sama. Lebih sering terjadi byte dikodekan merah dan kurang sering terjadi byte dikodekan dengan warna biru. Muatan pengulangan huruf a-i (ASCII 97105) jelas terlihat sebagai merah bar vertikal.



Bar vertikal di kisaran ASCII cetak (97-122). Garis vertikal menunjukkan nilai-nilai yang konstan antara paket, dalam banyak kasus ini adalah bidang header seperti versi IP (biasanya 4 untuk IPv4). Garis-garis diagonal menunjukkan nilai-nilai yang berubah pada tingkat yang konstan antara paket. Kemiringan garis menunjukkan arah dan laju perubahan. Keuntungan utama dari pandangan ini adalah kemampuan untuk membandingkan sampai dengan sekitar 1.000 paket pada satu waktu seperti kita hanya dibatasi oleh resolusi horisontal monitor. Teknik ini sebagian besar tergantung pada paket panjang sebagai paket yang lebih besar, bahkan lebih besar lagi.

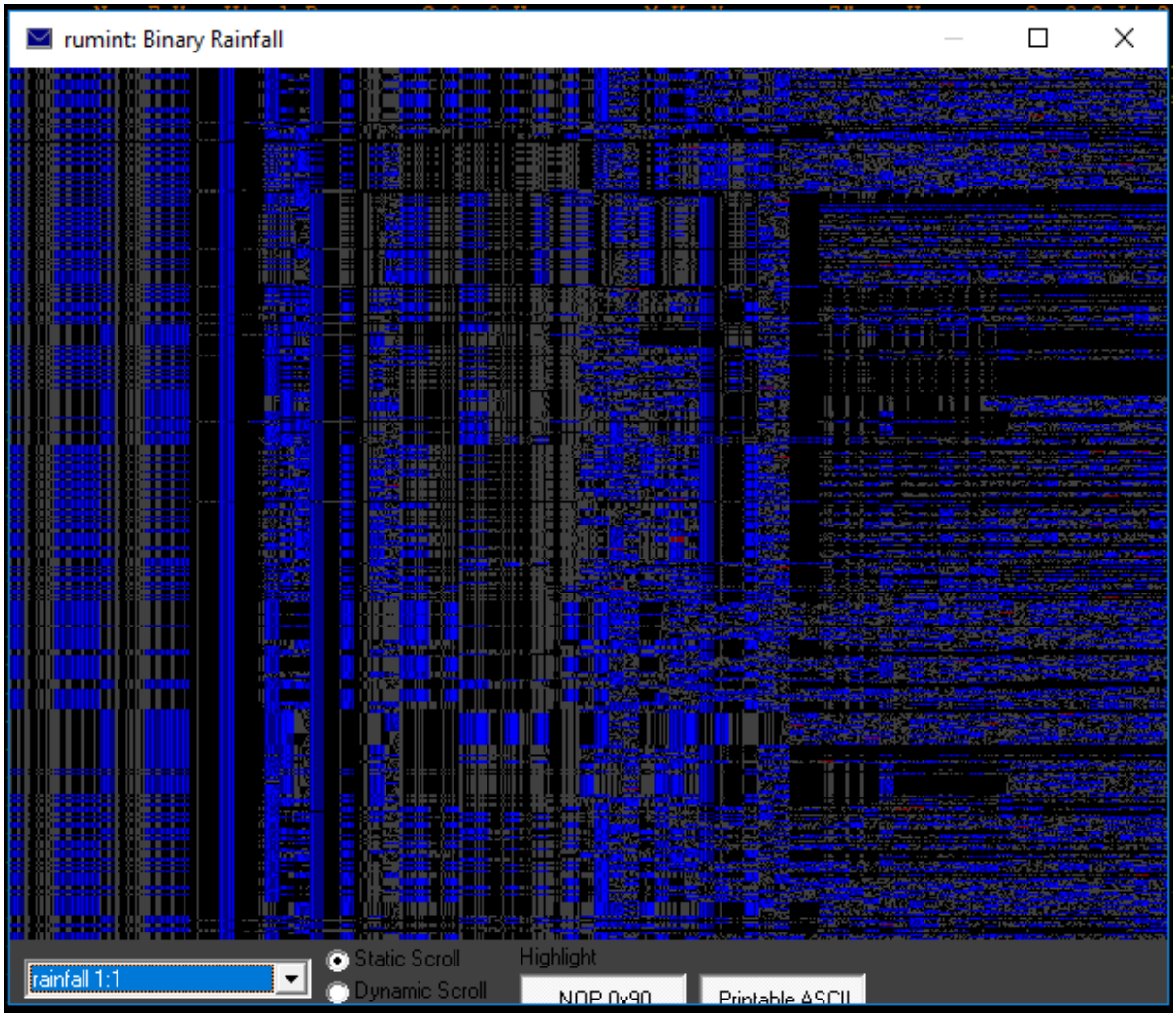
Gambar 5: A binary rainfall visualization dari paket ping yang sama. Satu paket per baris dan satu byte per pixel. Daerah header paket muncul di sebelah kiri setengah dari gambar sebagai piksel intermiten. Paket payload muncul sebagai gradien di sisi kanan dari gambar. Perhatikan bagaimana gradien restart seperti abjad diulang.



Batas Ethernet tradisional 1518 byte, dapat berisi hanya 256 bytes mungkin. Kerugian utama adalah hilangnya isi paket dapat dibaca manusia dan ketidakmampuan untuk melihat nilai byte yang terjadi lebih sering. Kita dapat mengatasi kekurangan ini kedua dengan color-coding pandangan oleh frekuensi byte bukan hanya ada atau tidaknya byte.

Gambar 4 menggambarkan paket ICMP sama tetapi mencakup ambang penyesuaian slider. Setiap byte (relatif terhadap paket tertentu) adalah kode warna merah (hot) untuk frekuensi yang lebih tinggi dan mereka yang jatuh di bawah ambang warna biru kode (dingin) untuk mereka frekuensi yang lebih rendah. Dengan menyesuaikan slider menjadi segera jelas bahwa bagian pertama dari huruf abjad terjadi lebih sering. Anda dapat mengkonfirmasi ini dengan mengambil melihat paket ICMP tekstual pada gambar 2. Kehadiran byte dan byte frekuensi pemandangan mengajukan pertanyaan. Apa sebenarnya yang menyebabkan garis-garis diagonal yang dapat dilihat di angka 3 dan 4? Untuk menjawab pertanyaan ini kita akan mengeksplorasi pandangan lain dari paket yang sama yang memberikan wawasan besar ke lokasi aktual (offset) byte dalam paket: curah hujan biner.

Gambar 6: A binary rainfall visualization dengan satu paket per baris dan satu bit per pixel. Daerah header paket muncul di sebelah kiri setengah dari gambar sebagai piksel intermiten. Paket payload muncul sebagai vertikal band di sisi kanan dari gambar. Nilai-nilai secara konsisten perubahan terjadi pada kolom yang ditandai (IP identifikasi Field), B (IP Header Checksum), C (ICMP Checksum), D (ICMP urutan nomor).



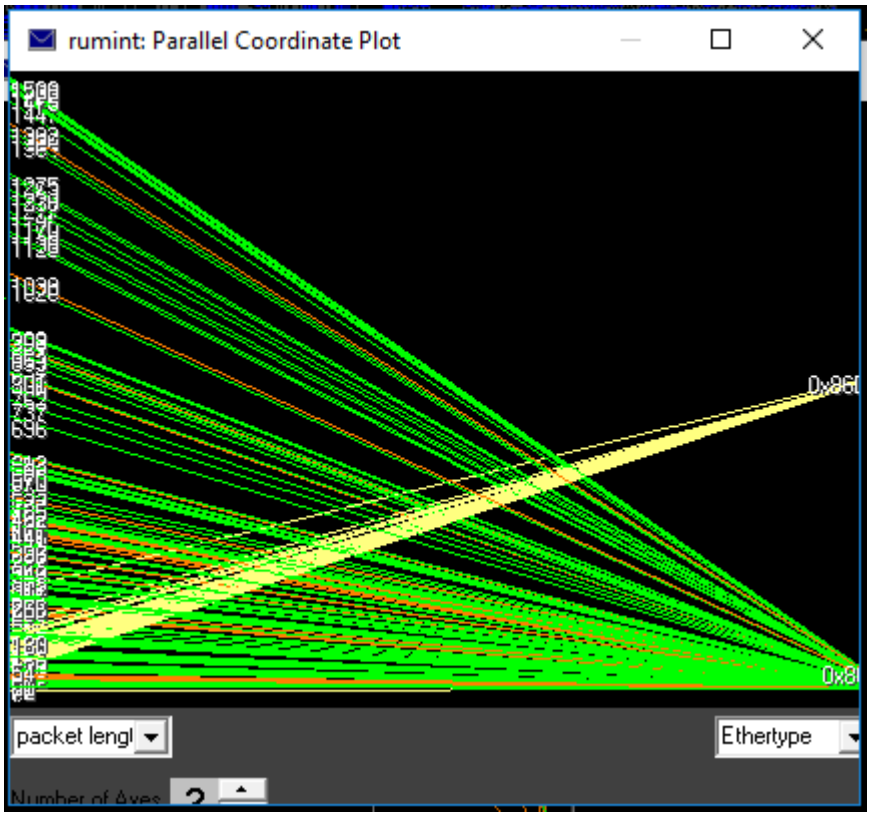
Curah hujan biner langsung peta nilai-nilai paket untuk piksel pada layar. Lagi ada satu paket per baris horisontal, tetapi setiap pixel diterangi berdasarkan nilai byte pada offset yang dalam paket. Untuk contoh jika paket nomor 50 memiliki nilai 42 pada posisi ke-100 dalam paket, di posisi 42, pixel 50 akan diterangi. Nilai sebenarnya dari byte (42) menentukan warna pixel. Byte memiliki 256 nilai yang mungkin sehingga tampilan curah hujan biner menggunakan tingkat 256

Warna skala, untuk menggambarkan isi paket. Dengan menggunakan teknik ini sebenarnya struktur paket dapat dilihat. Jika Anda memeriksa gambar 5 Anda akan melihat bidang header di sebelah kiri gambar, muncul sebagai piksel intermiten. Abjad muatan dapat dilihat di sebelah kanan. Gradien halus disebabkan oleh satu sampai perkembangan AZ., dan karenanya nilai-nilai byte. Perhatikan bagaimana gradien dimulai selama sebagai muatan abjad membungkus di sekitar dan dimulai lagi.

Visualisasi ini lagi memungkinkan Anda untuk membandingkan paket-paket sekitar 1.000 pada satu waktu dan lihat hampir seluruh paket. Anda akan memerlukan monitor dengan lebih dari 1518 bit resolusi horisontal untuk melihat paket terbesar. Perbedaan halus antara paket lebih keras untuk mendeteksi dan untuk mengidentifikasi penyebab garis diagonal kami menggunakan tampilan lebih rinci.

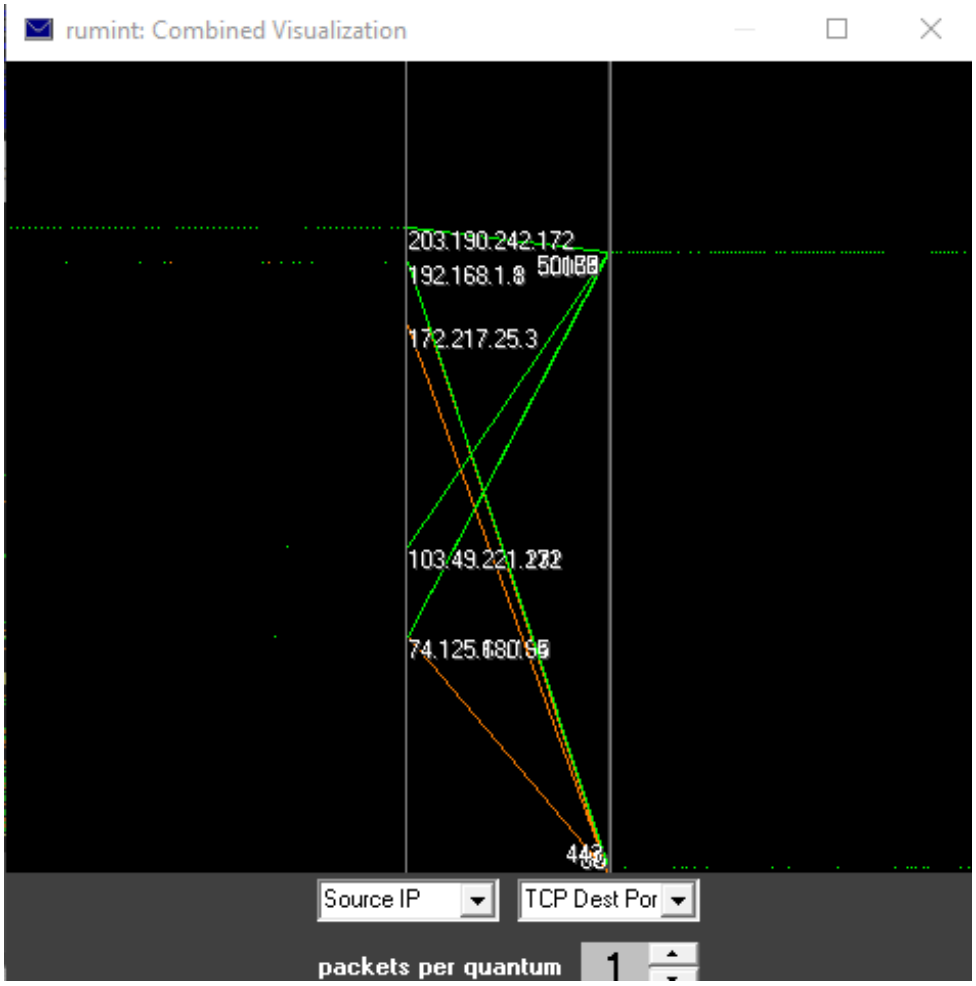
Untuk menciptakan yang lebih rinci pandangan kami menggunakan teknik yang sama, tetapi sebaliknya peta setiap bit dalam paket untuk sebuah pixel monokrom. Ini memotong paket seperti yang kita lihat hanya 1000 bit pertama dari setiap paket (~ 125 bytes), tetapi memungkinkan kita untuk melihat paket header jauh lebih rinci. Jika Anda mengambil lihat pada gambar 6 Anda akan melihat bahwa nilai-nilai konstan dan nilai-nilai secara konsisten perubahan yang mudah untuk mendeteksi. Nilai-nilai konstan bit yang muncul sebagai vertikal band dan nilai-nilai secara konsisten perubahan yang terlihat kira-kira seperti segitiga. Gambar 7 menunjukkan beberapa ratus paket ICMP. Dengan menggunakan tool yang Gunaka mouse di atas untuk menentukan posisi kolom yang mengandung segitiga daerah kita melihat bahwa mereka terjadi pada posisi 20, 26, 37 dan 41. Dengan menggunakan penganalisa protokol Ethereal kami mengkonfirmasi bahwa mereka adalah bidang identifikasi IP, IP Header Checksum, ICMP Checksum dan ICMP urutan nomor masing-masing.

Gambar 7: parallel coordinate plot memungkinkan dari 2 untuk sekitar 30 variabel dapat dibandingkan pada satu waktu. Gambar ini menunjukkan bahwa semua 500 Paket dalam ping dataset memiliki panjang identik, protokol ethertypes dan transportasi. Kita juga melihat bahwa hanya dua alamat IP dan dua nilai TTL yang hadir.



Sementara penganalisa protokol berbasis teks berguna untuk analisis paket-paket individu, visualisasi unggul menyediakan konteks gambaran besar. Saya ingin menggunakan plot koordinat paralel ketika pertama kali aku diberi file capture paket baru untuk menganalisis. Plot koordinat paralel memungkinkan dari 2 untuk sekitar 30 variabel dapat dibandingkan pada satu waktu. Konsep ini sederhana. Pertimbangkan gambar 8. Anda akan melihat bahwa ada delapan sumbu vertikal: paket panjang, ethertype, versi IP, TTL, IP transportasi protokol, sumber alamat IP, alamat IP tujuan dan IP fragmentasi bidang. Ini diambil dari bidang header setiap paket dan diplot pada setiap sumbu vertikal. Sebagai contoh, jika sebuah paket memiliki panjang 74, akan diplot pada sumbu pertama (paket panjang). Posisi vertikal diskala agar sesuai di layar. Dalam contoh ini 74 adalah sebagian kecil dari ukuran maksimum paket hukum dan dengan demikian muncul di dekat bagian bawah layar. Ada 500 Paket diwakili dalam gambar. Sekilas, kita bisa mengatakan bahwa mereka semua berbagi panjang paket sama (74 bytes), ethertype (0x800) dan menggunakan IP versi (IPv4) dengan fragmentasi tidak. Semua paket 500 digunakan hanya dua alamat IP dan dua nilai TTL (236 dan 128). Plot koordinat paralel berguna untuk cepat mencirikan set besar gambar paket dan menentukan bidang yang konstan, dekat konstan, acak dan berurutan, tetapi ia menderita satu kekurangan yang signifikan. Paket satu atau banyak dapat mengambil jalan yang sama dan sulit untuk membedakan. Sementara ada pendekatan yang dapat menangani oklusi cukup baik, seperti memudar remaja paket atau mengubah kecerahan untuk menunjukkan peningkatan aktivitas, sistem kami saat ini tidak memiliki kemampuan tersebut. Sebagai alternatif, kami akan menggunakan teknik visualisasi gabungan

Gambar 8: Visualisasi gabungan menggabungkan dua sumbu koordinat plot paralel dengan dua panel animasi. Setiap packet menghasilkan dua mesin terbang yang meluncur keluar dari layar. Dalam gambar ini sumber ping (192.168.1.100) menghasilkan aliran stabil ICMP paket semua dengan TTL 128, default Windows XP khas. Tanggapan intermiten kembali target (66.102.7.147) semua dengan TTL dari 236.



Visualisasi gabungan menggabungkan dua sumbu koordinat plot paralel dengan animasi glyphs untuk setiap paket. It mengatasi banyak masalah oklusi karena paket animasi dan pindah ke luar dari layar, seperti rudal pesawat ruang angkasa di asteroid. Sementara kita memilih untuk melihat alamat IP sumber dan membandingkannya dengan TTL, kotak dropdown di plot koordinat paralel tradisional (gambar 8) dan visualisasi gabungan (gambar 9) memungkinkan Anda untuk memilih fleksibel kumpulan bidang header yang berdasarkan kebutuhan Anda.

DAFTAR PUSTAKA

Conti, Greg. 2006. “RUMINT Imagery Analysis”. http://www.rumint.org. Diakses pada tanggal 5 September 2017.

Sofyan, M. Andre 2017. “Capturing Data dengan Wireshark”. http://edocs.ilkom.unsri.ac.id/cgi/users/home?screen=EPrint%3A%3AView&eprintid=1485. Diakses pada tanggal 4 September 2017.