Anggota Kelompok:

1. Ga tau berape - Johanes
2. 2501998845 – Jeremy Julian Tjang
3. 2540132723 – Immanuel Billy Christian Santoso
4. 2502008952 – Richard Marchelino Wijaya Tanzil, Tan

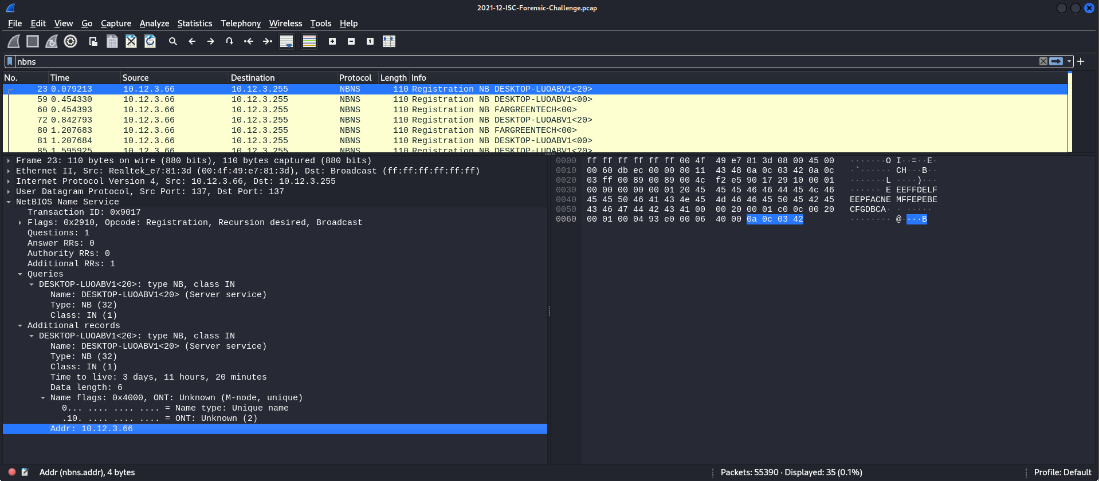
Berikut adalah Exercise yang kami pilih, **ISC December 2021 Forensic Challenge** yang mencakup tentang packet capture analysis on an Active Directory (AD) Environment.

|  |  |
| --- | --- |
| **Judul** | **ISC December 2021 : Forensic Challenge** |
| **Link** | <https://isc.sans.edu/diary/December+2021+Forensic+Contest+Answers+and+Analysis/28160> |

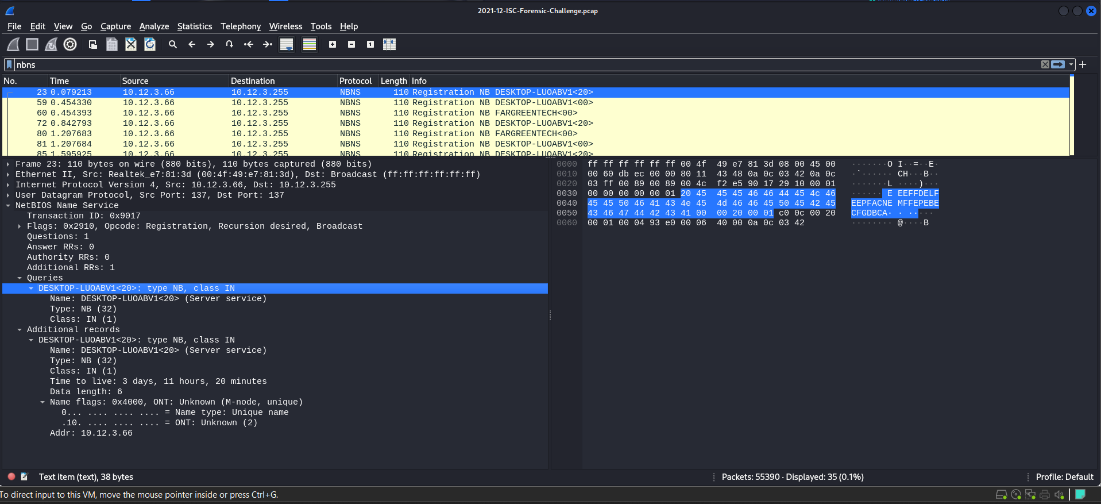
**Questions:**

1. Apa IP address dari Windows Computer yang terinfeksi malware?
2. Apa Host name dari Windows Computer yang terinfeksi malware?
3. Apa nama user account dari Windows Computer yang terinfeksi malware?
4. Kapan tanggal dan waktu infeksi malware ini terjadi?
5. Apa Family dari Malware yang menginfeksi Windows Computer ini?

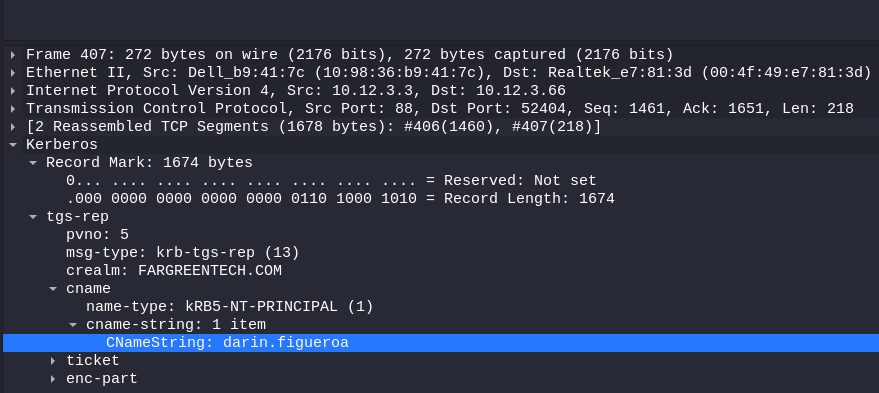
**Soal 1,** membutuhkan kita untuk mencari IP Address dari komputer window yang terinfeksi dengan malware. Untuk mendapatkan IPnya ada beberapa cara yang bisa dilakukan untuk memfilter file pcap yang ada. Untuk kasus ini filter “NBNS” digunakan, lalu muncullah satu komputer yang bernama “DESKTOP-LUOABV1”. Ketika kita membuka detail terhadap salah satu transaksi yang ada kita bisa mendapatkan “Addr” yaitu IP Address device windows tersebut yaitu **“10.12.3.66”.**



**Soal 2,** Jawaban untuk soal ini sudah di jawab dari soal sebelumnya yaitu **“DESKTOP-LUOABV1”**.



**Soal 3,** Untuk mengerjakan soal ini kami kembali lagi menggunakan filter terhadap pcap file yang ada. Kami perlu memfilter Kerberos traffic yang biasanya muncul ketika seorang user membuka *active directory.* Filter yang kami pakai untuk ini adalah “kerberos.CNameString”. Dan kami mendapatkan username **“darin.figueroa”**



**Soal 4 & 5,** untuk menajwab kedua soal ini, pertama kita harus melakukan Analisa lebih mendalam pada packet yang ada, dimana kitab isa lihat disitu ada 2 GET Request dari web yang terlihat cukup aneh, yaitu pada :

* **gamaes.shop/wp-content/plugins/sSTToaEwCG5VASw**
* **newsaarctech.com/wp-content/Sx9tvV5**

U,{baec835a-5268-42d6-965d-085636e2968e}{131},3.125,3.125

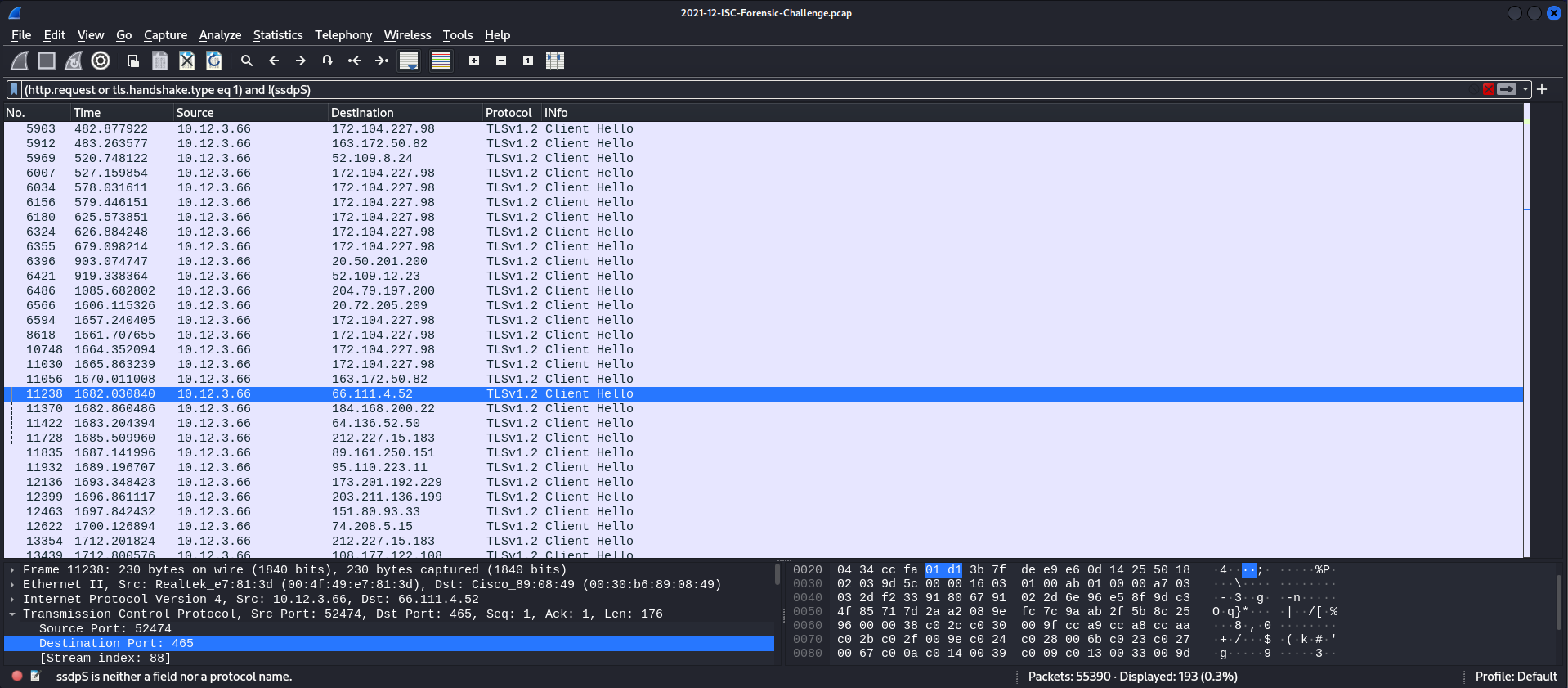
Dari 2 website ini cika kita coba melakukan checking di google ternyata beberapa sumber telah menyatakan bahwa kedua website ini menghosting DLL files untuk malware **Emotet**, untuk soal nomor 5, jawabannya adalah dari family **Emotet**, ada banyak referensi yang bisa dicantumkan tapi saya akan list beberapa saja:

* <https://urlhaus.abuse.ch/url/1844646/>
* <https://cyberint.com/blog/research/emotet-returns/>
* <https://labs.k7computing.com/index.php/diving-into-the-emotet-maldoc-boutade/>

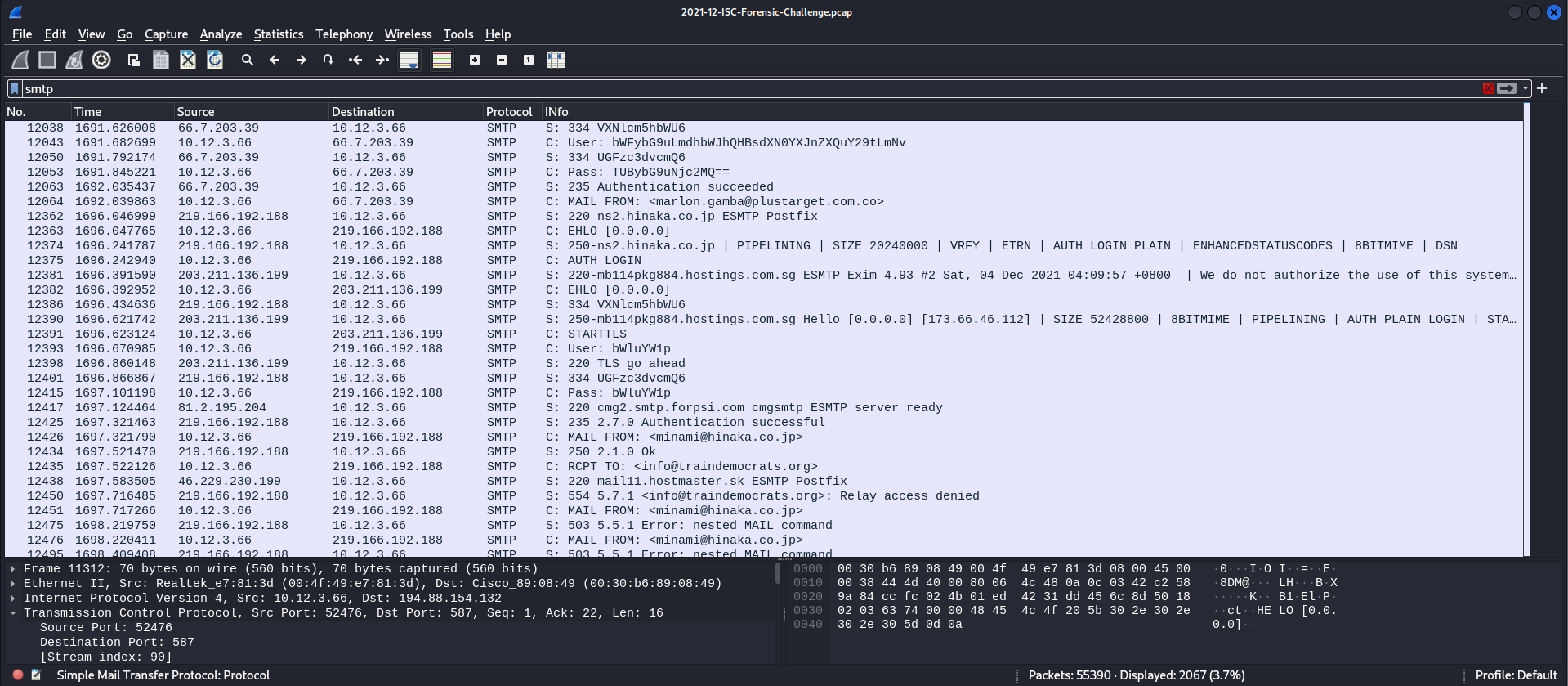
Dikutip dari <https://feodotracker.abuse.ch/> ditemukan bahwa ada 2 address yang berjalan di TCP yang menjadi C2 Channels untuk Emotet malware ini

* 172.104.227.98 port 443
* 163.172.50.82 port 443

Jika kita amati terus menggunakan filter seperti ini **(http.request or tls.handshake.type eq ) and !(ssdp)** kitab isa langsung melihat bahwa tiba-tiba setelah port 443 ada port lain yaitu port 465 dan port 587, dan jika kita lihat waktu mulainya ini akan menjawab pertanyaan kita untuk soal nomor 4, di kapan serangan malware ini bermulai.



Lanjut lagi karena kita sudah tahu ini ada di port-port ini, kita akan lanjut mencari lagi dengan filter **smtp** karena di port yang tadi digunakan adalah port yang merepresentasikan SMTP traffic, dan ternyata disalah satu capture package di **2021-12-03 20:09:57 89.161.250.151** dapat dilihat ada info yang menuliskan “TCP Spurious Retransmition” hal ini terjadi Ketika sebuah paket di transmisikan ulang walaupun sudah di “Acknowledge” oleh yang penerima



Kalau kita Analisa lebih dalam dengan filter **smtp.data.fragment** kita bisa lihat ada 17 file email yang tertangkap dan dikirim tanpa enkripsi via SMTP protocol, kita lalu bisa mendownload email – email ini dengan menggunakan **file -> Export Objects -> IMF**

