Nama : Gonewaje
NIM : 09011181419005

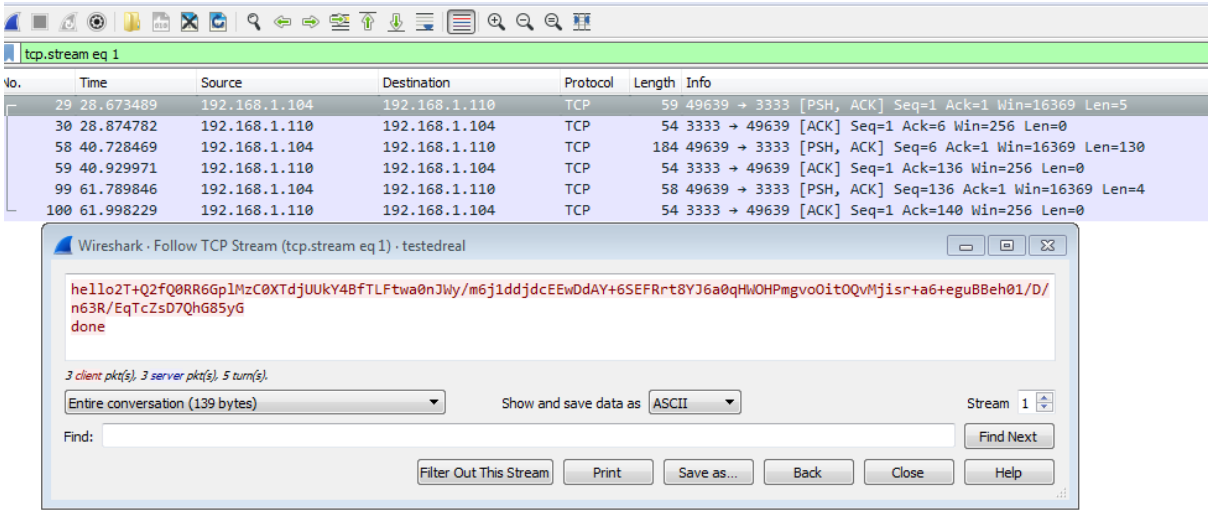
Audio Forensic

Ilmu forensik adalah sebuah penerapan dari berbagai ilmu pengetahuan untuk menjawab pertanyaan-pertanyaan yang penting untuk sebuah sistem hukum yang mana hal ini mungkin terkait dengan tindak pidana. Namun disamping keterkaitannya dengan sistem hukum, forensik umumnya lebih meliputi sesuatu atau metode-metode yang bersifat ilmiah (bersifat ilmu) dan juga aturan-aturan yang dibentuk dari fakta-fakta berbagai kejadian, untuk melakukan pengenalan terhadap bukti-bukti fisik (contohnya mayat, bangkai, dan sebagainya).

Pada kesempatan kali ini kita akan melakukan sebuah kasus forensik sederhana dimana kasus yang akan kita bahas adalah mengenai forensik audio, yang mana forensik audio atau suara meruapakan bagian dari macam-macam ilmu forensik dalam dunia komputer seperti halnya forensik dalam file, forensik dalam gambar, forensi dalam video, forensik dalam audio-video dan masih banyak lagi.

Kasus ini kita misalkan ada sebuah badan forensik nasional yang sedang melakukan penyelidikan terhadap dua orang yang diduga melakukan bisnis ilegal, badan forensik ini melakukan sniffing diberbagai alat komunikasi yang mereka gunakan dan didapatlah data .pcap sebagai berikut yang mana pada paket ke-29 didapat sebuah percakapan yang sebagian percakapan tersebut telah terenkripsi

Nama : Gonewaje
NIM : 09011181419005



Dapat dilihat pada gambar diatas bahwa diduga tersangka 1 dengan source **IP 192.168.1.104** mengirimkan sebuah pesan kepada diduga tersangka 2 dengan destination **IP 192.168.1.110.** Saat dilakukan Follow TCP Stream pada paket yang dicuriga ternyata terdapat pesan yang sebagiannya tidak ‘human readable’, yang dapat kita baca secara normal hanya lah ‘hello’ dan ‘done’ selebihnya mungkin telah terenkripsi. Teknik enkripsi dalam dunia komputer sudah tidak asing lagi digunakan untuk menjaga kerahasiaan dari paket/pesan yang dikirimkan, untuk melalukan enkripsi/decode pesan acak tersebut kita gunakan website yang banyak menyediakan layanan enkripsi/decode secara gratis, tinggal feeling kita mencoba satu persatu teknik enkripsi mana yang dilakukan oleh diduga tersangka tersebut untuk mengenkripsi pesan mereka, didapat hasil sbb:

Encrypted Text

```
2T+Q2fQ0RR6GplMzC0XTdjUUkY4BfTLFtwa0nJWy/m6j1ddjdcEEwDdAY+6SEFRrt8YJ6a0qHW
OHPmgvoOitOQvMjisr+a6+eguBBeh01/D/n63R/EqTcZsD7QhG85yG
```

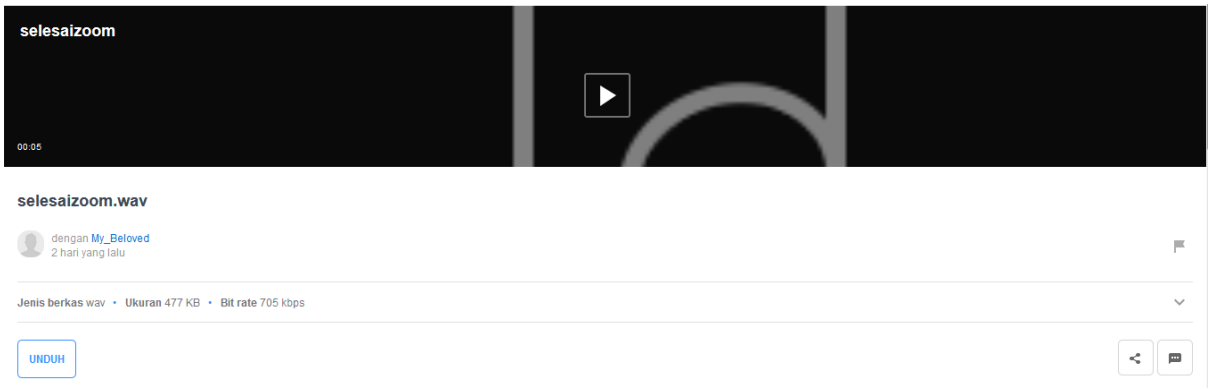
Decrypt

Decrypted Text

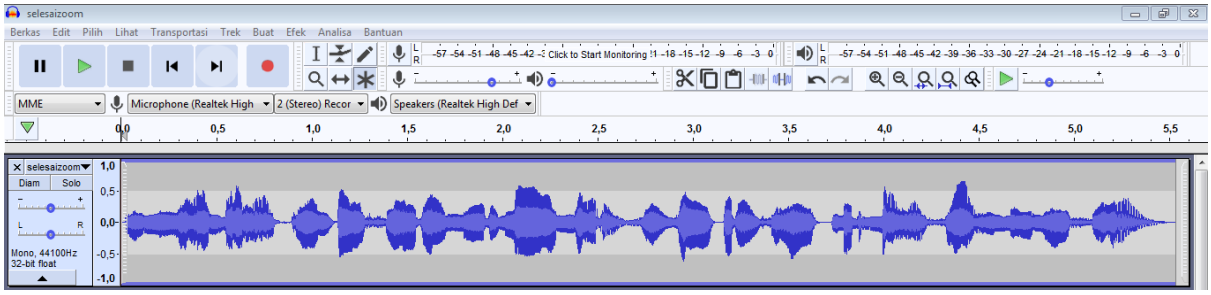
```
download audio ini : https://www.4shared.com/music/s9DIdv2tei
/selesaizoom.html

kunci : 0.0000-0.0030, morse
```

Nama : Gonewaje
NIM : 09011181419005

Dari pesan tersebut dapat disimpulkan bahwa diduga tersangka tersebut menginstruksikan kepada diduga tersangka 2 untuk mendownload file audio dengan address yang tersedia serta disertai pula kunci yang mungkin kunci untuk membaca file audio tersebut.

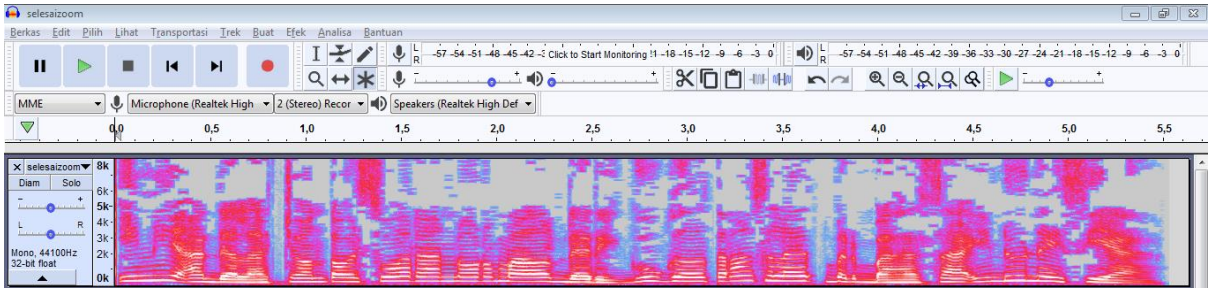


Pada gambar diatas terlihat tampilan halaman download file yang dimaksud oleh diduga tersangka 1. Apabila file tersebut kita buka pada aplikasi audio seperti contohnya Audacity dan kita dengarkan audio tersebut adalah : ‘Ini adalah contoh suara normal dari google translate berbahasa Indonesia’



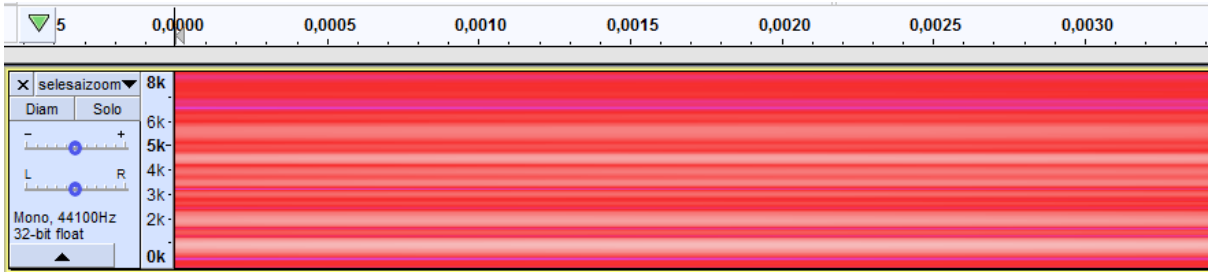
Sekilas tidak ada yang aneh dari suara tersebut, hanya suara bot oleh laman google translate yang diputar kemudian disimpan dalam bentuk file audio .wav, tapi jangan lupa pada pesan terenkripsi yang kita dapatkan sebelumnya bahwa disana ada kunci yaitu :
Kunci : 0.0000-0.0030, morse

Sekarang coba kita aktifkan *Spectogram* pada Audacity karena teknik ini sangat banyak digunakan untuk menyembunyikan pesan.

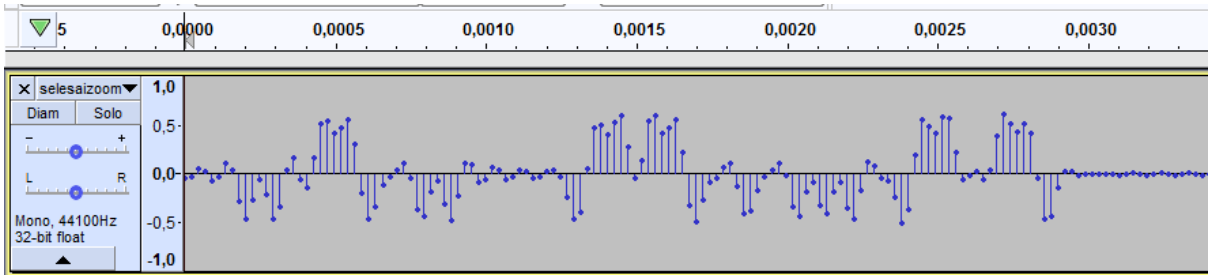


Kemudia dilakukan zoom untuk melihat pada waktu **0.0000-0.0030** apakah ada pesan tersembunyi yang dimaksud

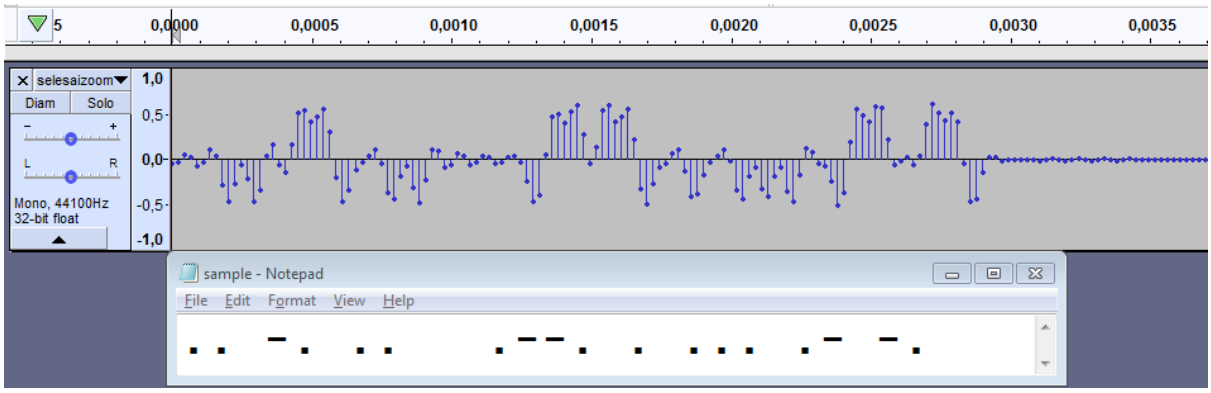
Nama : Gonewaje
NIM : 09011181419005



Kemungkinan tidak ada, kita kembalikan ke mode Waveform



Terdapat sebuah pola yang tidak alami pada audio atau gelombang audio/suara pada umumnya dan jika didengarkan pun hanya menghasilkan noise sedikit saja pada awal suara padahal suara yang direkam adalah suara dari bot, kembali kita lihat kunci sebelumnya yaitu kata **Morse**, apabila kita coba dengan pencocokan dengan sandi morse seperti tanda titik (**.**) dan tanda garis strip (-) didapatkan hasil sbb :



Kembali kita gunakan website penyedia encode decode morse dan akhirnya kita melihat isi pesan tersebut yaitu :