Laporan Penyisihan 2 – Gemastik 8 Jaringan

Dibuat oleh : Psycho Security

Anton Salim (672011055)

Aditya Wicaksana (672012226)

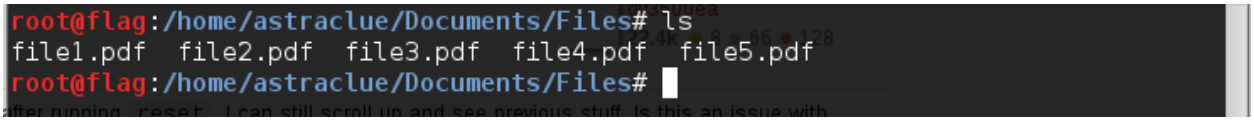
Dhimas Wiharjo (672011205)

Fakultas Teknologi Informasi

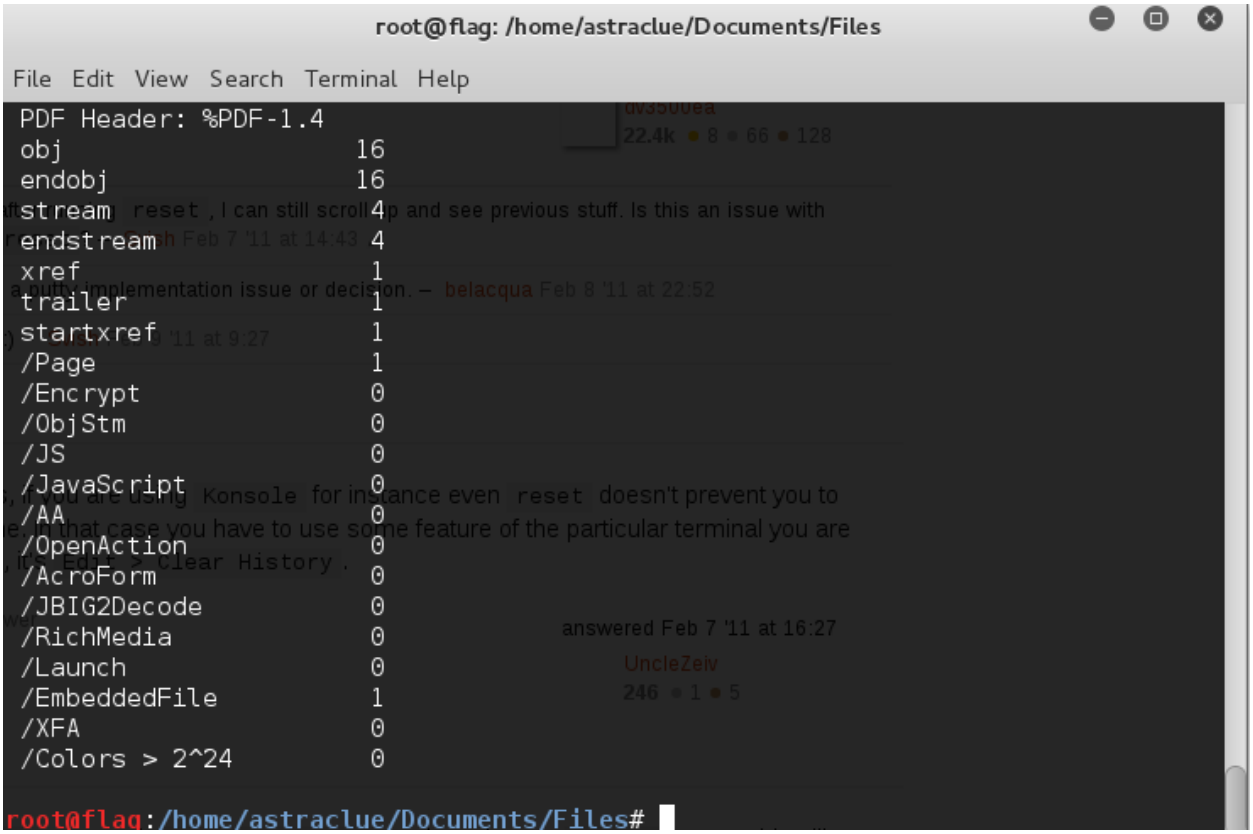
Universitas Kristen Satya Wacana

Soal A

Pada soal ini kita mendapatkan 5 buah file pdf.

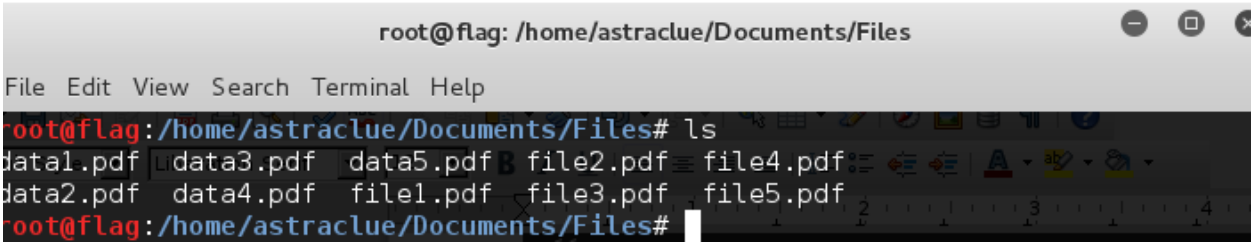


Terdapat file1.pdf, file2.pdf, file3.pdf, file4.pdf, dan file5.pdf.



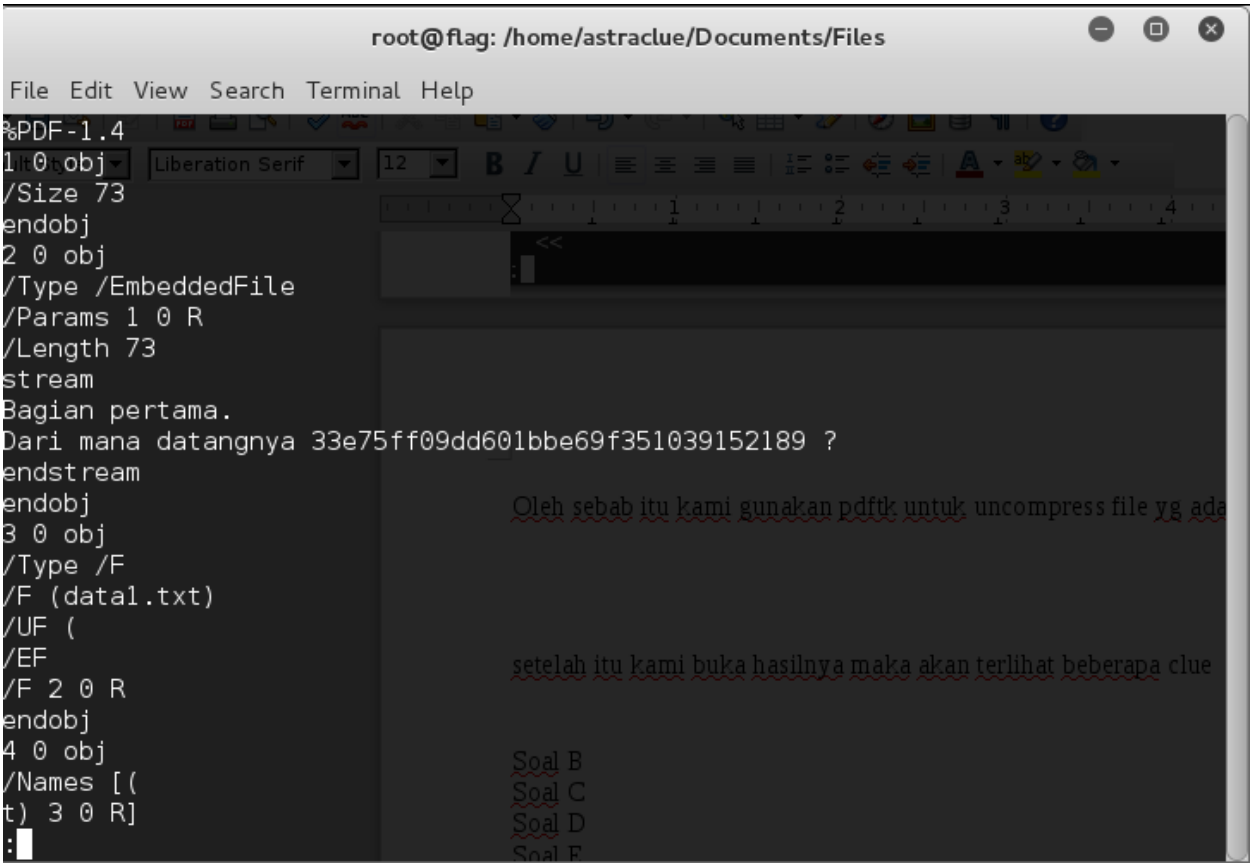
Kita menggunakan pdfid dan ternyata ada file embed di dalam file tersebut.

Oleh sebab itu kami gunakan pdftk untuk uncompress file yg ada di pdf1 sampai pdf5 menjadi sebagai berikut :



Setelah itu kami buka hasilnya maka akan terlihat beberapa hash yang terdapat di dalam file – file pdf tersebut :

Clue pdf1 ada hash sebagai berikut “33e75ff09dd601bbe69f351039152189”.



Clue pdf 2

Bagian Dua.

Dari mana datangnya ea0f3b9271eff45033bea3a6b1c36fa0000c3de7 ?

Clue pdf 3

Bagian Tiga.

Dari mana datangnya a9bcf1e4d7b95a22e2975c812d938889 ?

Clue pdf 4

Bagian Empat.

Dari mana datangnya 1489eec1dd6f153d2da7d5a4b40bc078896fc006c8534dc449ce35e28436fd6a ?

Clue pdf 5

Bagian Terakhir.

Dari mana datangnya 44c582df70cc6e653adf2cf0df3f29fd1b6e16ca ?

Setelah kami analisis sepertinya menggunakan hash cluenya maka saya check dengan hash-identifier untuk menyakinkan kembali ternyata benar menggunakan hash.

Hash 1 : md5

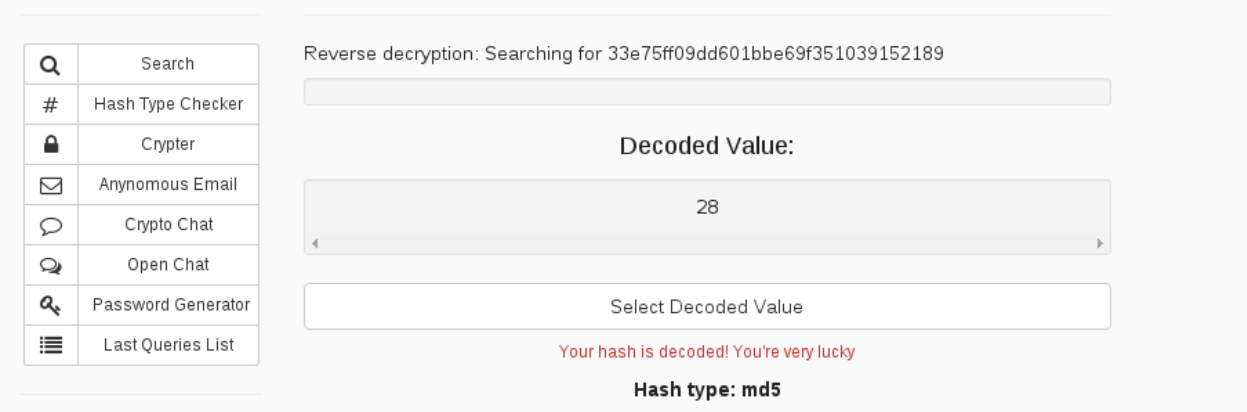
Hash 2 : sha1

Hash 3 : md5

Hash 4 : sha256

Hash 5 : sha1

Kami menggunakan decoder online sesuai hash yang digunakan seperti md5hasing.net atau hashkiller.co.uk untuk mendeskripssikan maksud clue tersebut.



Hasilnya sebagai berikut :

Clue 1 : 28

Clue 2 : okt

Clue 3 : hari

Clue 4 : sumpah

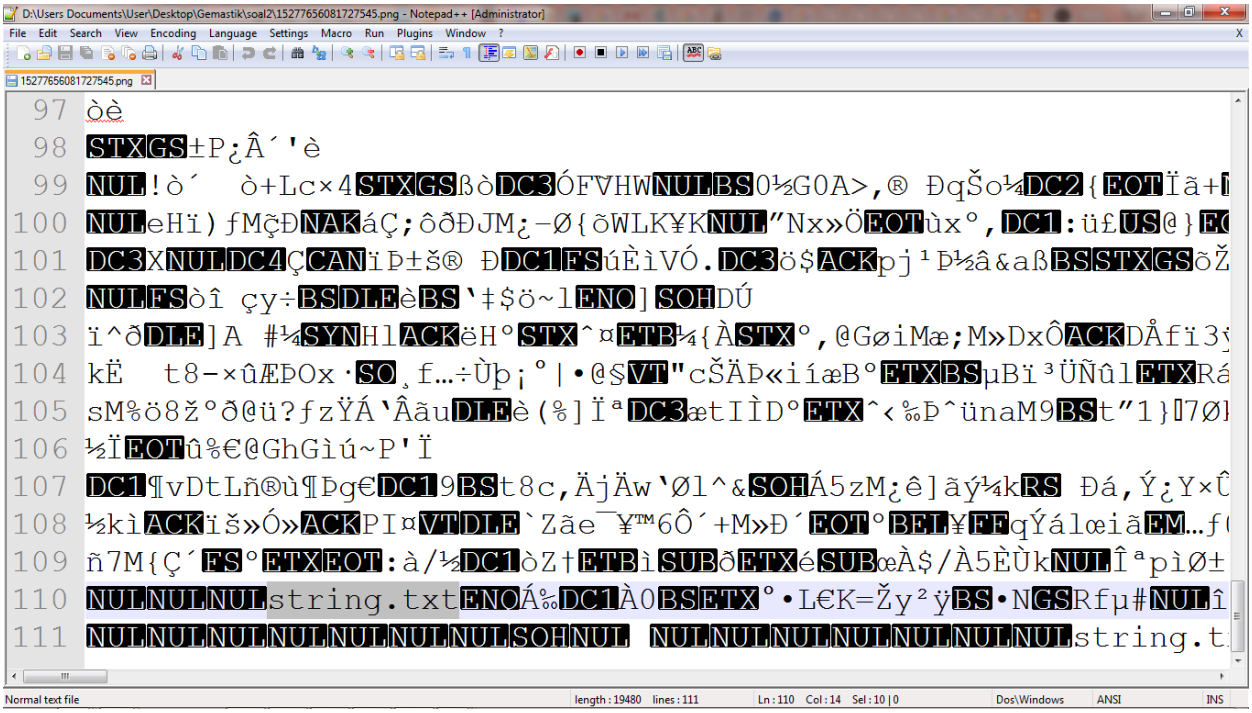
Clue 5 : ...?

Kalo melihat dari cluenya yang sudah ditemukan akan menjadi ***28 okt hari sumpah … ?***

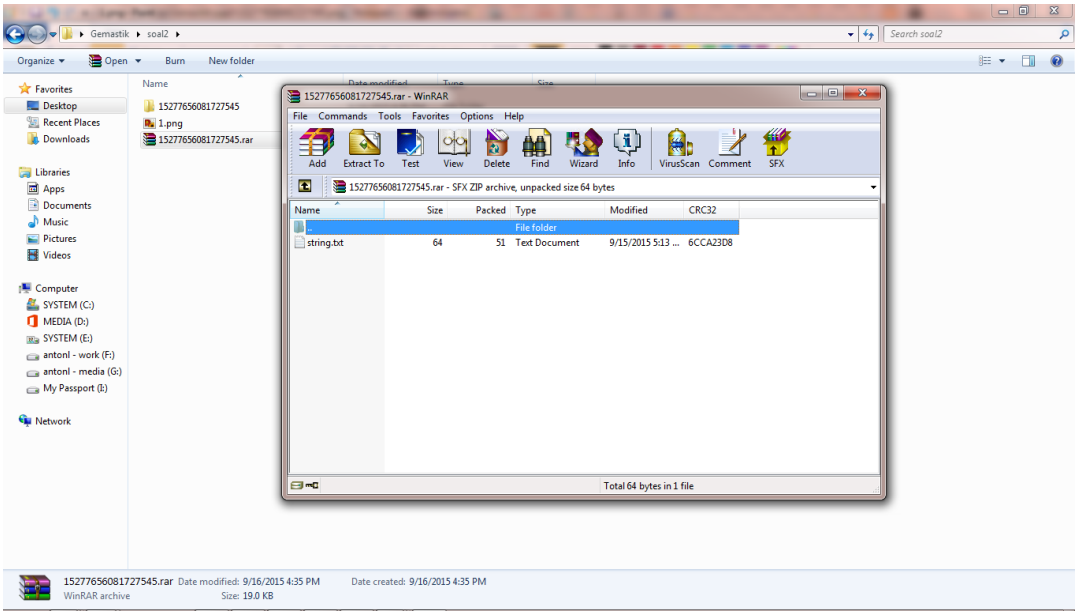
Awalnya kita tidak menemukan clue 4, kita mencoba submit dengan “sumpahpemuda” berulang – ulang, ternyata jawabannya hanya “pemuda”.

Soal B

Dalam soal ini kita diminta untuk mengunduh file gambar yang bernama “15277656081727545.png”. Karena tidak ada clue lain, kita mecoba membukanya dengan notepad file tersebut.

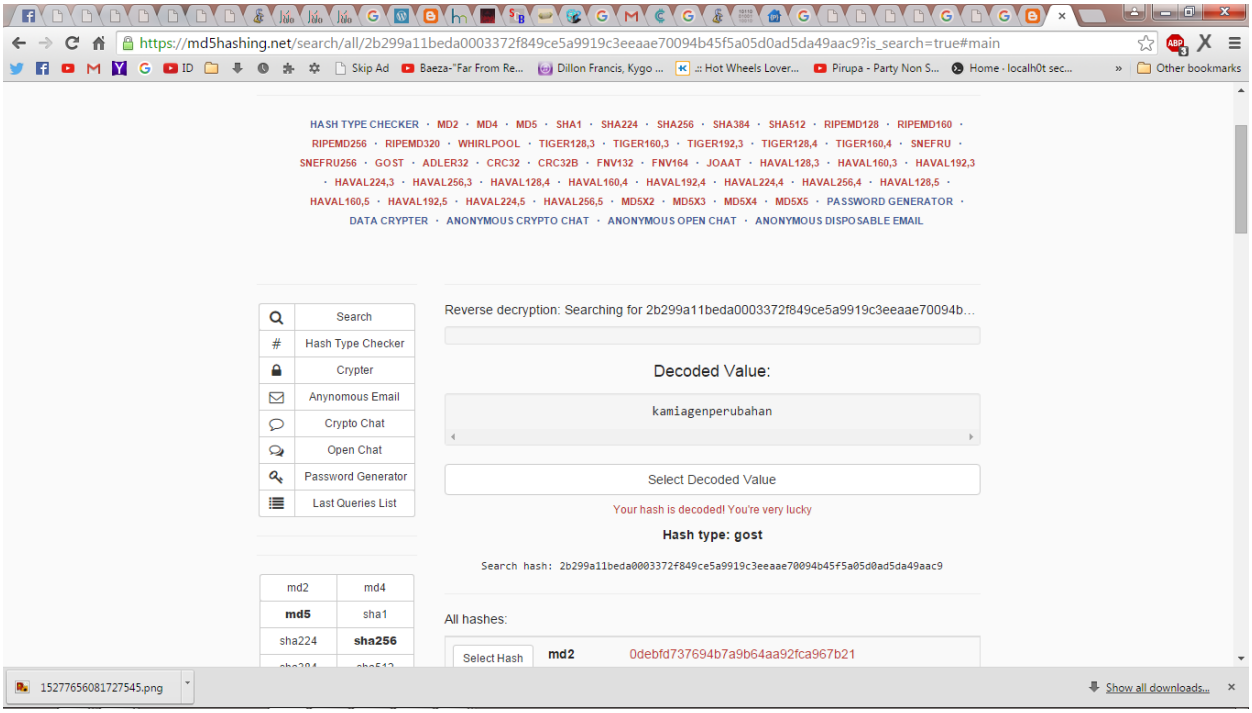


Disini kita melihat di baris 110, kita mencurigai ada file “string.txt”.



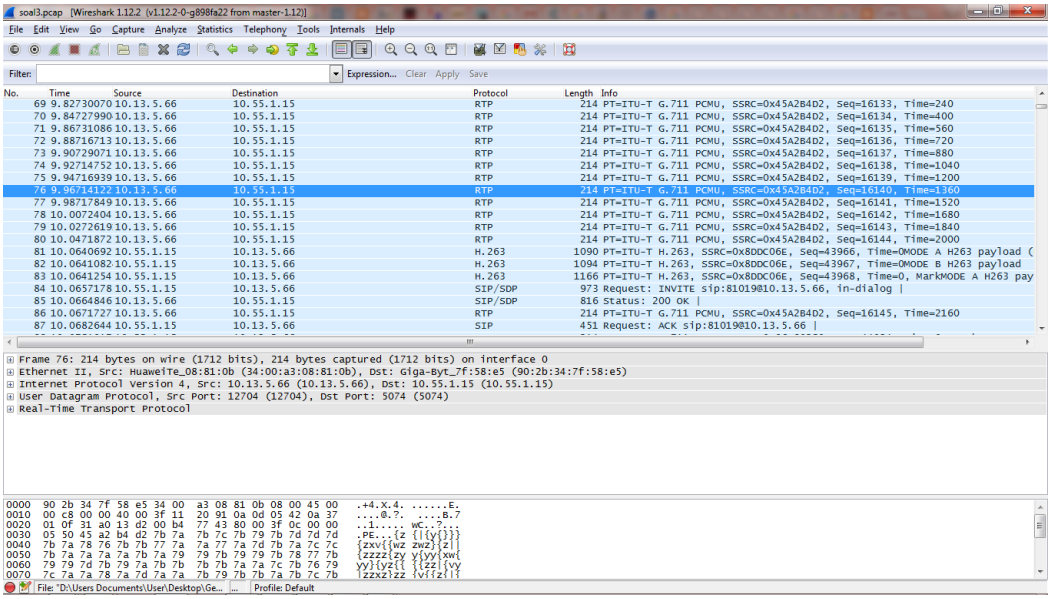
Setelah mencobanya kita mengubah format file beberapa kali, ternyata file .rar lalu kita extract file tersebut dan menemukan file string.txt

Isi dalam file string.txt berupa hash “2b299a11beda0003372f849ce5a9919c3eeaae70094b45f5a05d0ad5da49aac9”.

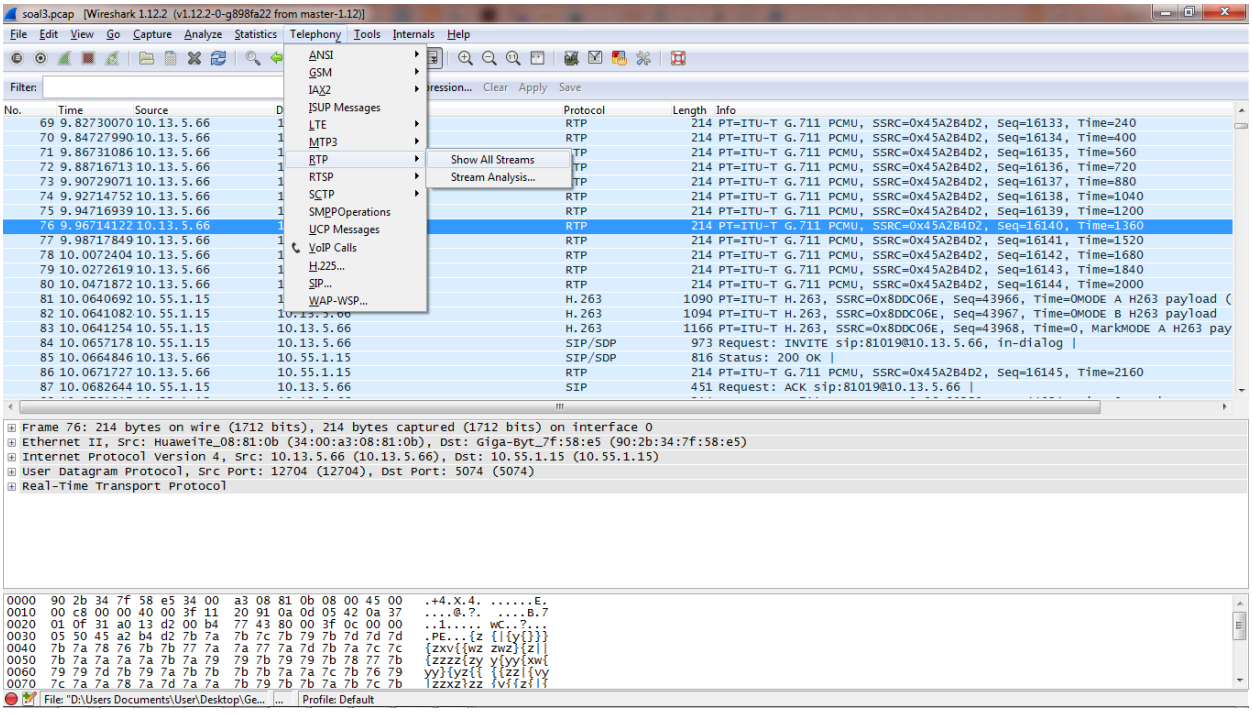


Kita menyelesaikan dengan menggunakan tools online “md5hashing.net” untuk memecahkannya dan ternyata setelah di decode diketahui jawabannya “kamiagenperubahan” yang merupakan hasil dari hash type : gost.

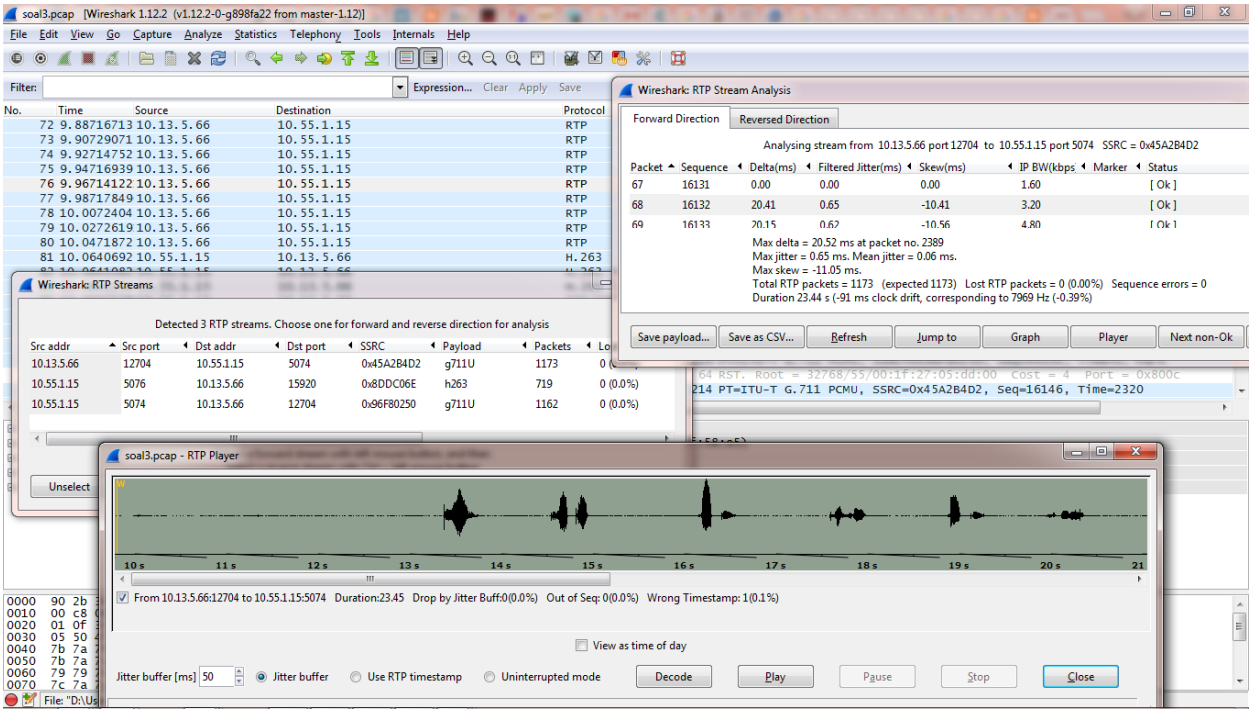
Soal C



Pada soal ini kami mendapatkan file “soal3.pcap”, setelah dibuka dengan wireshark kita melihat ada banyak protocol RTP.



Kita mencoba membuka streams untuk mencari tahu apakah ada percakapan yang terjadi dalam soal file .pcap ini. Telephony > RTP > Show All Streams.



Setelah itu kami menemukan ada file yang bisa di analyze, kita mencoba membuka file tersebut dan ada pesan angka yang disampaikan “2810192828102015”. Angka tersebut merupakan jawaban dari soal ini.

Soal E

Pada soal ini kita mendapatkan clue “fun crypto”, dan ternyata ada 3 baris dan memiliki berbeda jenis.

Geser sedikit dong ...

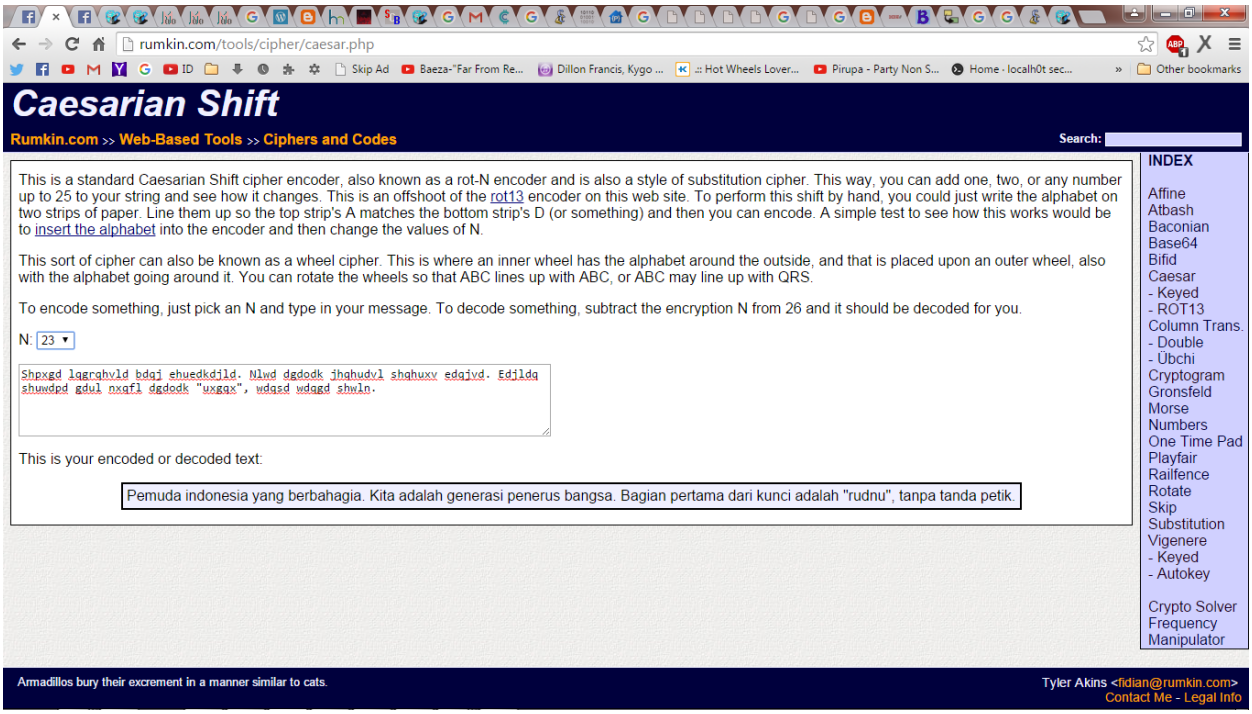
Shpxgd lqgrqhvld bdqj ehuedkdjld. Nlwd dgdodk jhqhudvl shqhuxv edqjvd. Edjldq shuwdpd gdul nxqfl dgdodk "uxgqx", wdqsd wdqgd shwln.

Butuh kunci untuk membuka pesan.

lyek iuo 1000 btixa gwi, xcfeiiu nmix eheilog umwyew lklv csklaai. lyek iuo 10 cguexn pqcwnai kenp seahpkkhtmix xhpqk. vniqkh xgleu qczs ehpks uqctkb "zivknacx", duari duafi zygks

Bekerja keras untuk memenuhi kebutuhan keluarga (diperibahasakan)

Yztrzm gvizpsri wzir pfmxr zwzozs "hfivgfqzn" gzmkz gzmwz kvgrp.



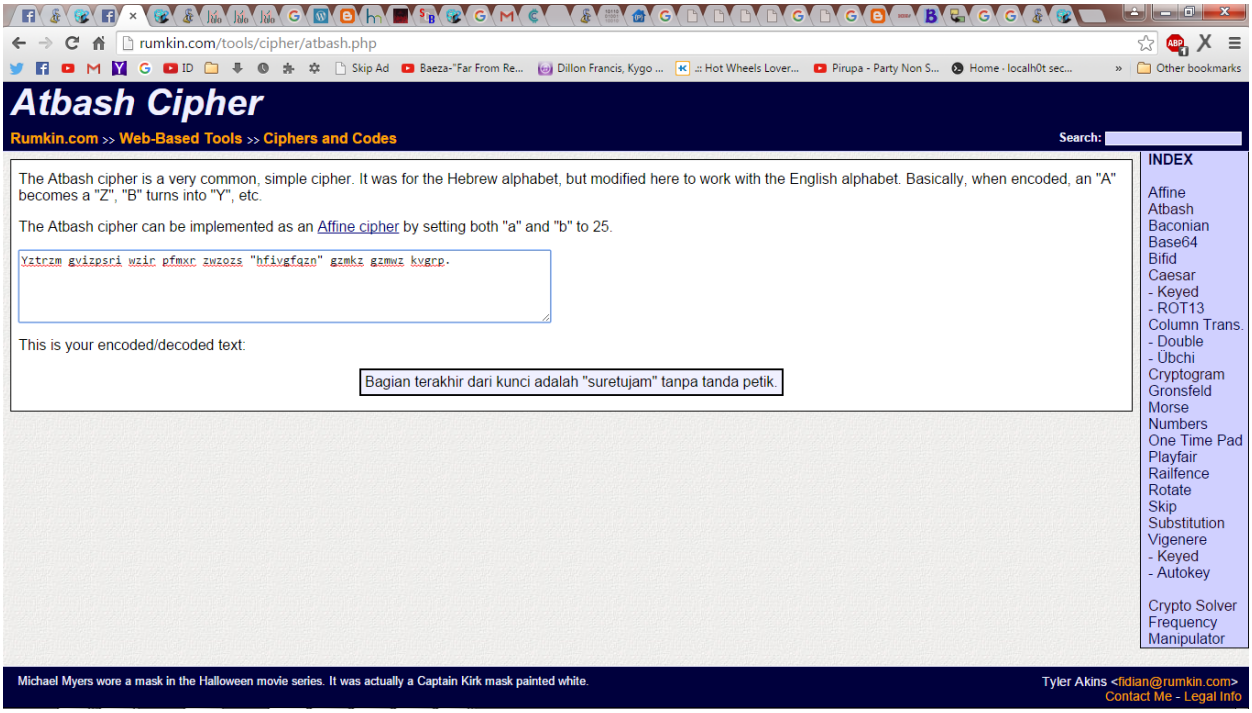
Pada baris pertama kita mengerjakan menggunakan tools online dari rumkin.com

“Shpxgd lqgrqhvld bdqj ehuedkdjld. Nlwd dgdodk jhqhudvl shqhuxv edqjvd. Edjldq shuwdpd gdul nxqfl dgdodk "uxgqx", wdqsd wdqgd shwln.” Merupakan Caesarian Shift yang digeser 23.

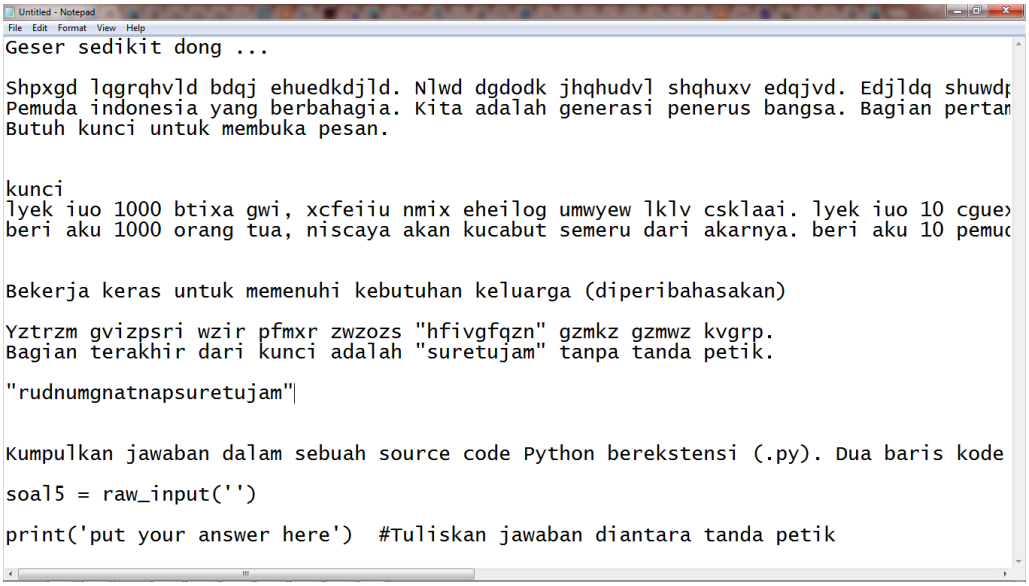
Hasilnya “Pemuda indonesia yang berbahagia. Kita adalah generasi penerus bangsa. Bagian pertama dari kunci adalah "rudnu", tanpa tanda petik.”

Pada baris kedua “lyek iuo 1000 btixa gwi, xcfeiiu nmix eheilog umwyew lklv csklaai. lyek iuo 10 cguexn pqcwnai kenp seahpkkhtmix xhpqk. vniqkh xgleu qczs ehpks uqctkb "zivknacx", duari duafi zygks” yang merupakan Keyed Vignere Ciphere dan kita mendapatkan clue “butuh kunci untuk membuka pesan”.

Hasilnya “beri aku 1000 orang tua, niscaya akan kucabut semeru dari akarnya. beri aku 10 pemuda niscaya akan kuguncangkan dunia. bagian kedua dari kunci adalah "mgnatnap", tanpa tanda petik” di decrypt dengan Passphrase “kunci”.



Pada baris ketiga “Yztrzm gvizpsri wzir pfmxr zwzozs "hfivgfqzn" gzmkz gzmwz kvgrp.” yang merupakan Atbash Cipher. Setelah di decode “Bagian terakhir dari kunci adalah "suretujam" tanpa tanda petik.”.



Dari hasil semua decode terdapat kata yang direverse dalam tanda “, kita coba gabungkan kita menemukan hasil “majuteruspantangmundur”. Setelah mencoba submit jawaban ternyata salah, tetapi jawabannya memang tetap reverse yaitu “rudnumgnatnapsuretujam”.