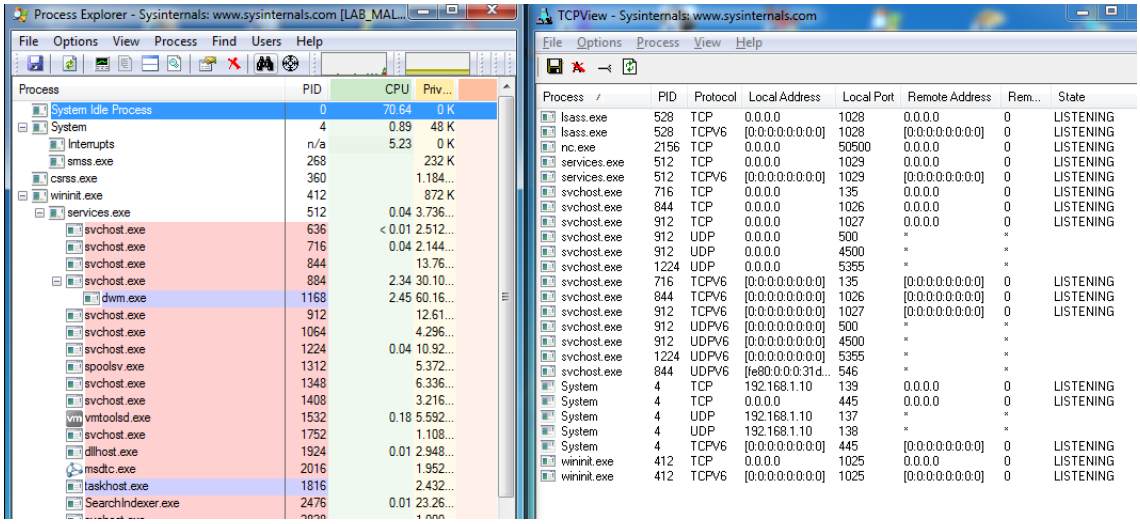
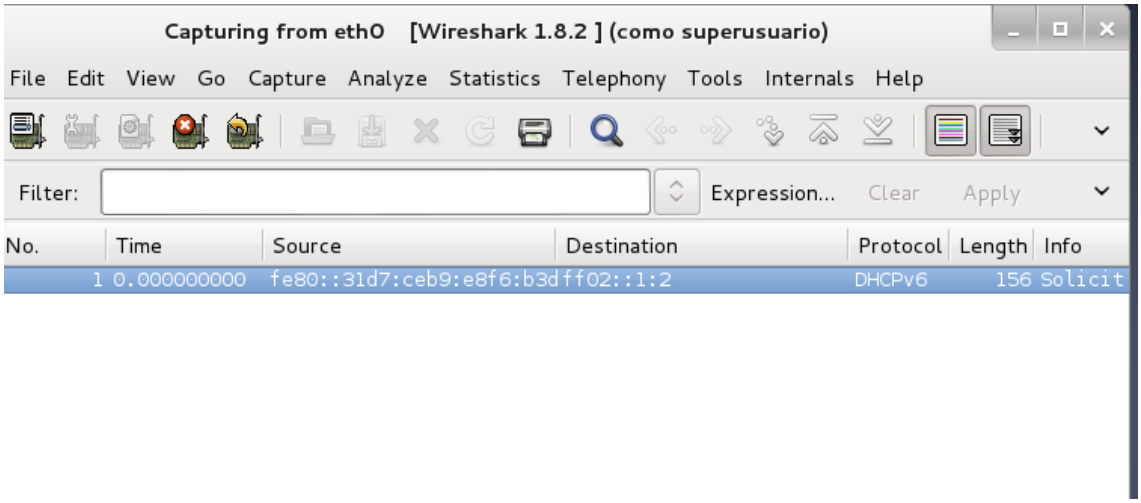
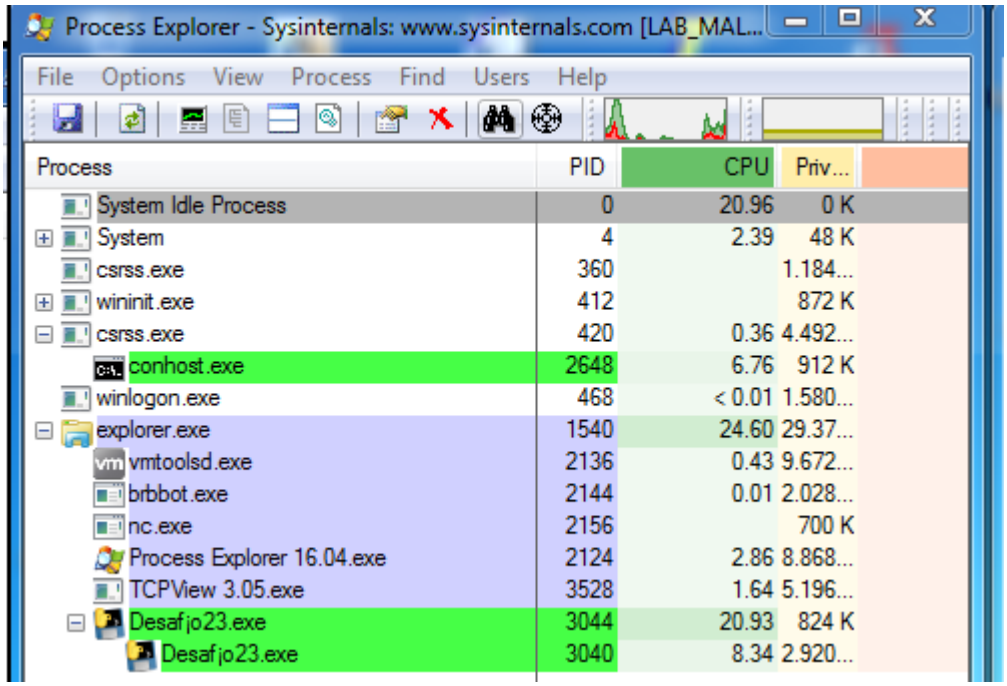
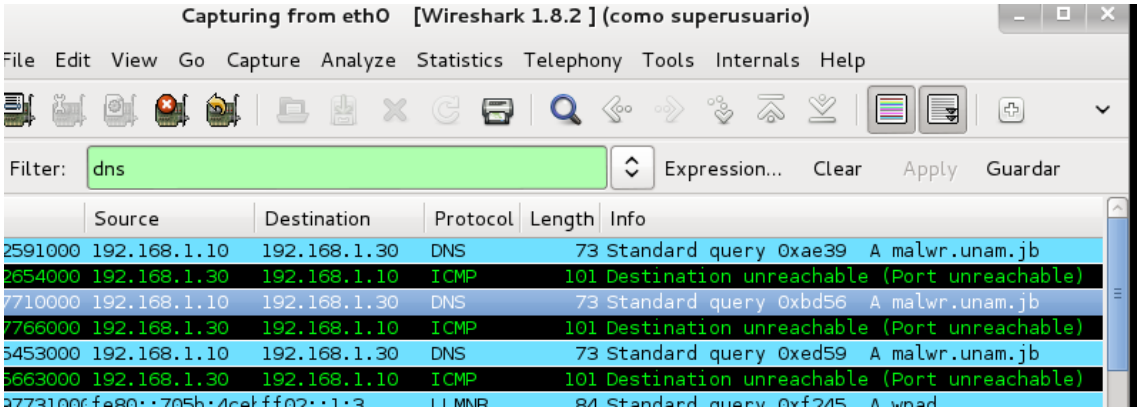
Analisis de Malware
Gonzalo Vazquez Cruz
413038357
Tarea 5

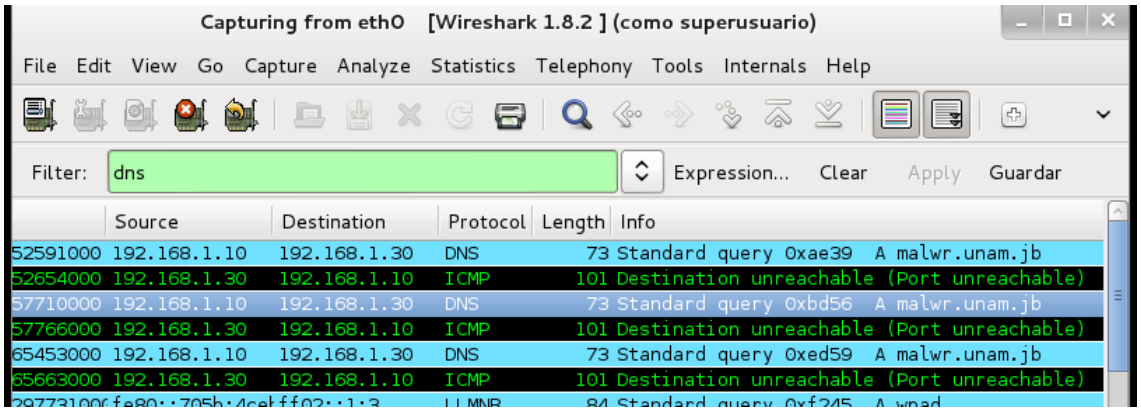


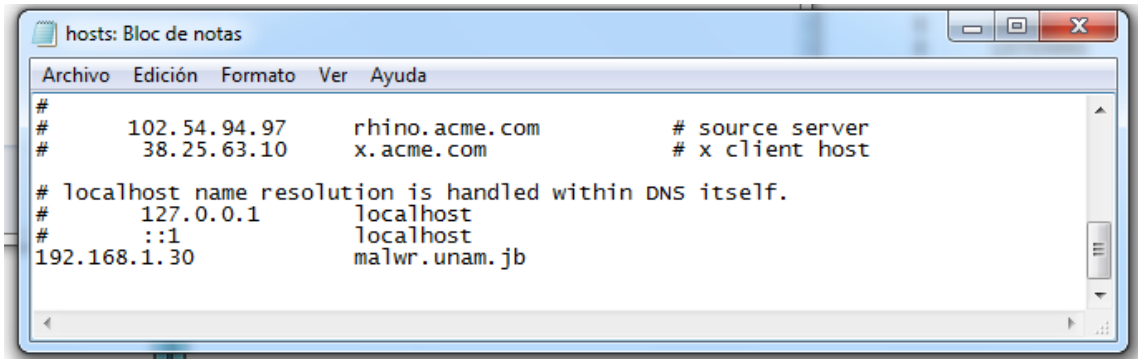




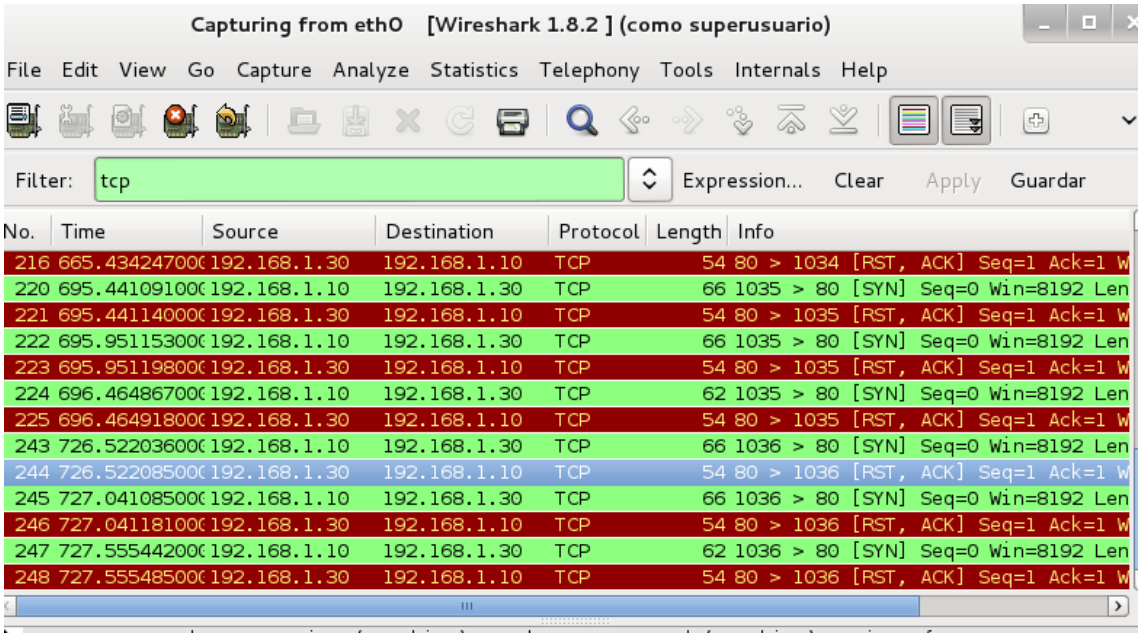
Analisis de Malware
Gonzalo Vazquez Cruz
413038357
Tarea 5

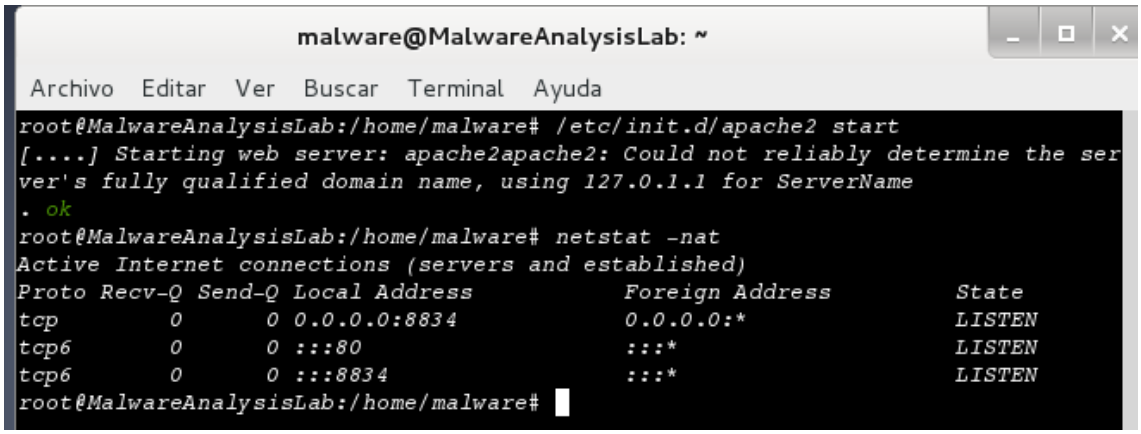


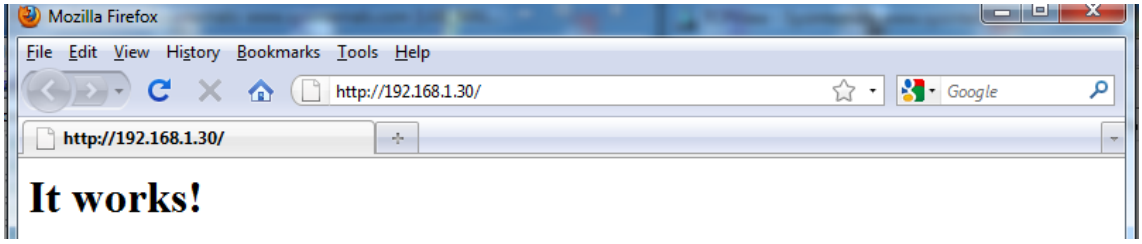


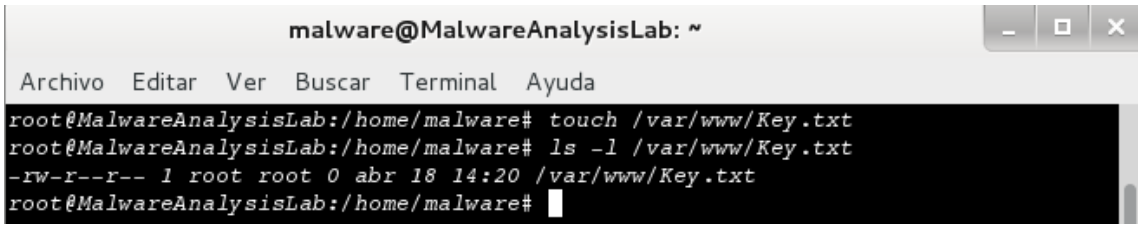


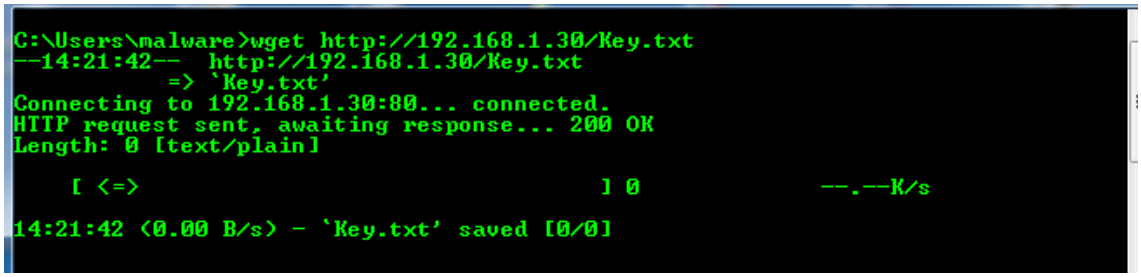
Analisis de Malware
Gonzalo Vazquez Cruz
413038357
Tarea 5

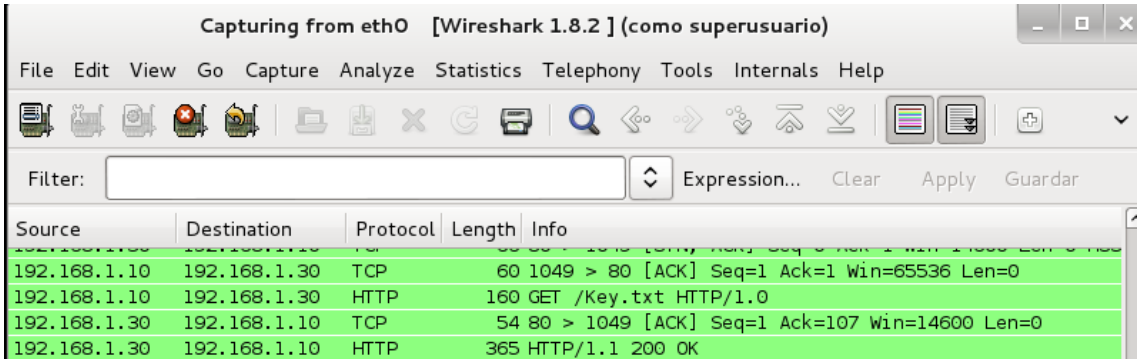


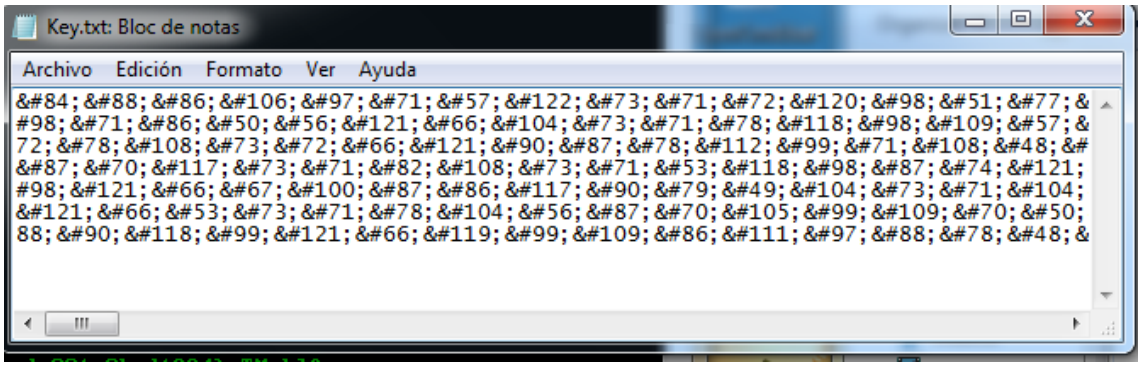


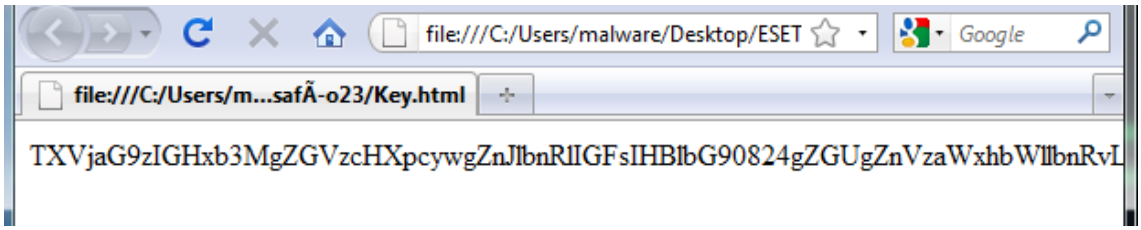


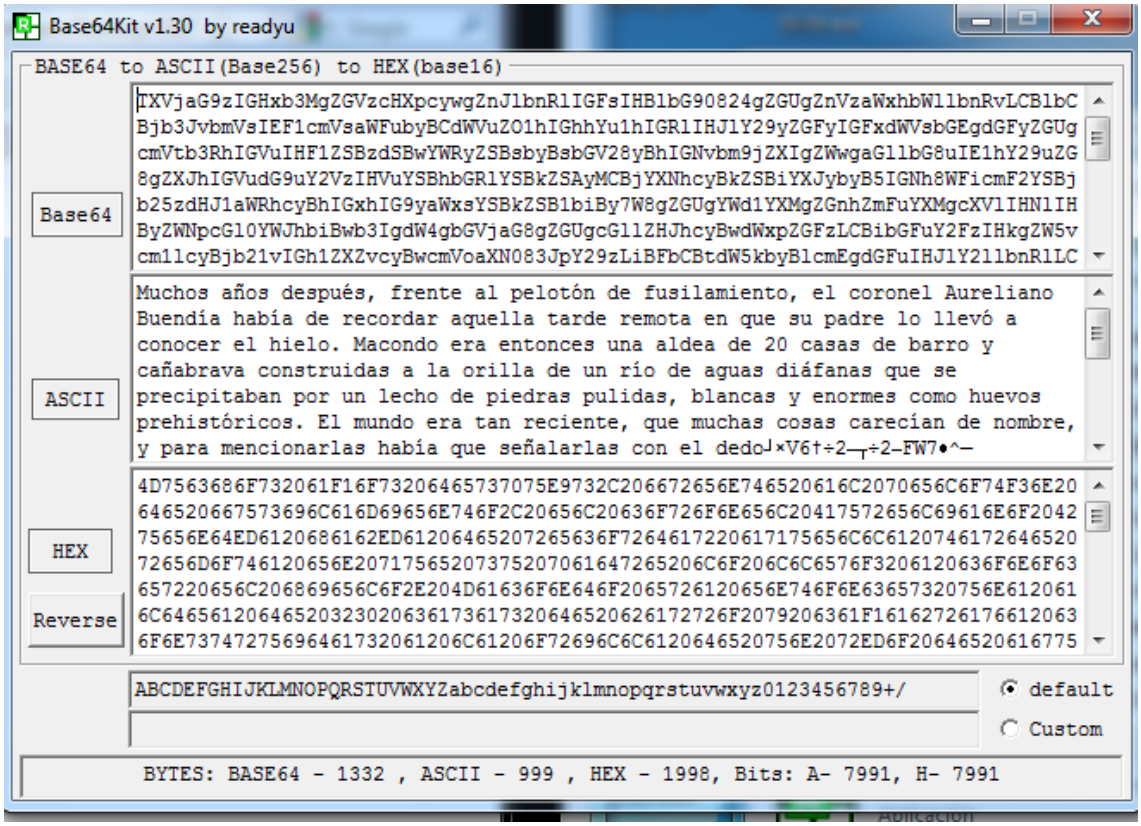



C:\Users\malware>wget http://192.168.1.30/Key.txt
--14:21:42-- http://192.168.1.30/Key.txt
=> 'Key.txt'
Connecting to 192.168.1.30:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 0 [text/plain]
[<=>] 0 --.--K/s
14:21:42 (0.00 B/s) - 'Key.txt' saved [0/0]


Capturing from eth0 [Wireshark 1.8.2] (como superusuario)
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Guardar
Source Destination Protocol Length Info
192.168.1.10 192.168.1.30 TCP 60 1049 > 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
192.168.1.10 192.168.1.30 HTTP 160 GET /Key.txt HTTP/1.0
192.168.1.30 192.168.1.10 TCP 54 80 > 1049 [ACK] Seq=1 Ack=107 Win=14600 Len=0
192.168.1.30 192.168.1.10 HTTP 365 HTTP/1.1 200 OK


Key.txt: Bloc de notas
Archivo Edición Formato Ver Ayuda
TXVjaG9zIGHxb3M&
#98;GV28yBhIGNvbm9&
72;NlIHByZWNpcGl0&#
WFuIGRlIG5vbWJy
#98;yBCdWVuZO1hIGh
yB5IGNh8WFicmF2
88;ZvcyBwcmVoaXN0&


file:///C:/Users/malware/Desktop/ESET
Google
file:///C:/Users/m...safÃ-o23/Key.html
TXVjaG9zIGHxb3MgZGVzcHXpcywgZnJlbnRlIGFsIHBlbG90824gZGUgZnVzaWxhbWllbnRvL


Base64Kit v1.30 by readyu
BASE64 to ASCII(Base256) to HEX(base16)
Base64
TXVjaG9zIGHxb3MgZGVzcHXpcywgZnJlbnRlIGFsIHBlbG90824gZGUgZnVzaWxhbWllbnRvLCBlbC
Bjb3JvbmVsIEF1cmVsaWFubyBCdWVuZO1hIGhhYu1hIGRlIHJlY29yZGFyIGFxdWVsbGEgdGFyZGUg
cmVtb3RhIGVuIHF1ZSBzdSBwYWRyZSBsbyBsbGV28yBhIGNvbm9jZXIgZWwgaGllbG8uIE1hY29uZG
8gZXJhIGVudG9uY2VzIHVuYSBhbGRlYSBkZSAyMCBjYXNhcyBkZSBiYXJybyB5IGNh8WFicmF2YSBj
b25zdHJ1aWRhcyBhIGxhIG9yaWxsYSBkZSB1biBy7W8gZGUgYWd1YXMgZGnhZmFuYXMgcXVlIHNlIH
ByZWNpcGl0YWJhbiBwb3IgdW4gbGVjaG8gZGUgcG11ZHJhcyBwdWxpZGFzLCBibGFuY2FzIHkgZW5v
cm1lcyBjb21vIGh1ZXZvcyBwcmVoaXN083JpY29zLiBFbCBtdW5kbyBlcmEgdGFuIHJ1Y2llbnRlLC
Muchos años después, frente al pelotón de fusilamiento, el coronel Aureliano
Buendía había de recordar aquella tarde remota en que su padre lo llevó a
conocer el hielo. Macondo era entonces una aldea de 20 casas de barro y
cañabrava construidas a la orilla de un río de aguas diáfanas que se
precipitaban por un lecho de piedras pulidas, blancas y enormes como huevos
prehistóricos. El mundo era tan reciente, que muchas cosas carecían de nombre,
y para mencionarlas había que señalarlas con el dedo
ASCII
HEX
4D7563686F732061F16F73206465737075E9732C206672656E746520616C2070656C6F74F36E20
646520667573696C616D69656E746F2C20656C20636F726F6E656C20417572656C69616E6F2042
75656E64ED6120686162ED6120646520726 36F726461722061717 5656C6C6120746172646520
72656D6F746120656E2071756520737520706164726 206C6F206C6C6576F3206120636F6E6F63
657220656C206869656C6F2E204D61636F6E646F2065726120656E746F6E63657320756E612061
6C6465612064652032302063617361732064652062617272 6F2079206361F161627261761 2063
6F6E737472756964617320612061206C61206F72696C6C6120646520756E2072ED6F20646520616775
Reverse
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
default
Custom
BYTES: BASE64 - 1332 , ASCII - 999 , HEX - 1998, Bits: A- 7991, H- 7991