If at first, you don't succeed, try something else

Jim Clausing, PMTS and SANS Instructor
jac@att.com
jclausing@isc.sans.edu

AT&T

Agenda

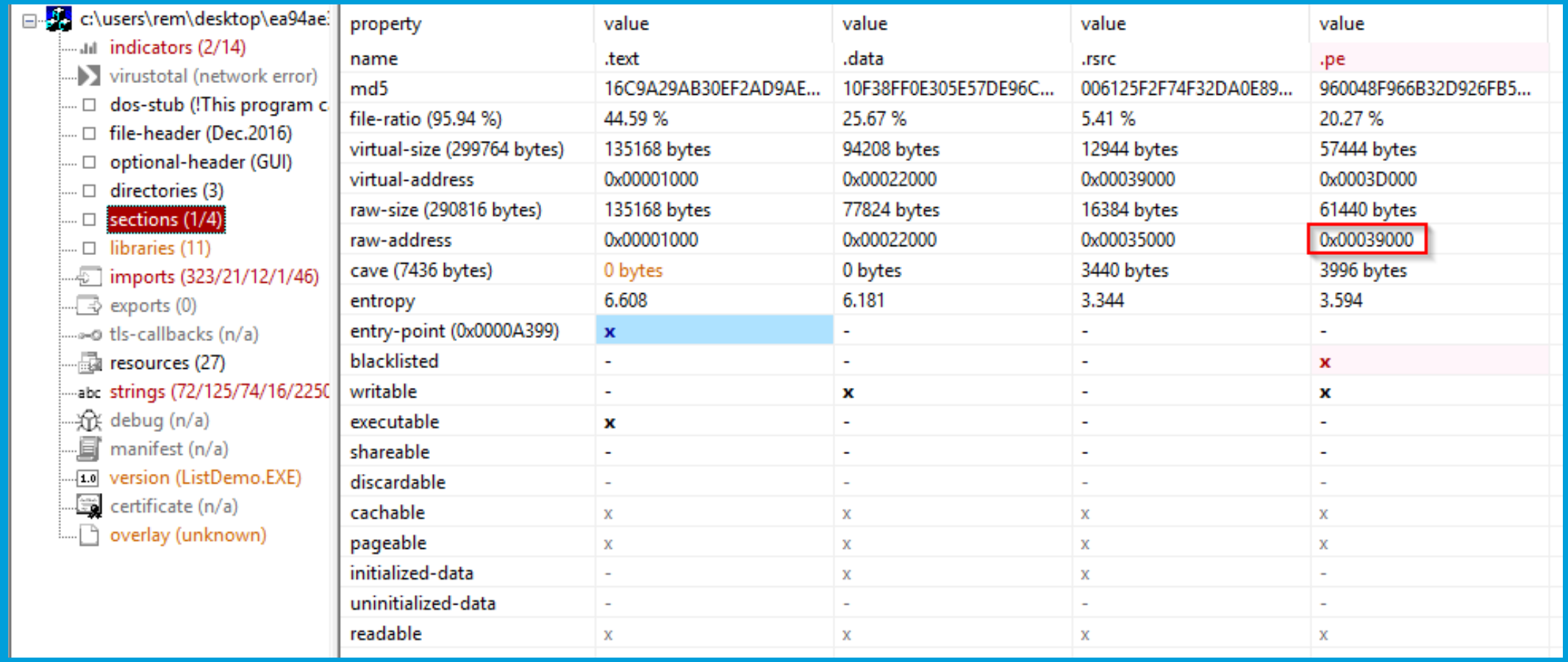
1: Intro
2: The Analysis
3: Questions

Forensicator, Malware analyst, SANS instructor, Cyclist, Private pilot

The start of the hunt

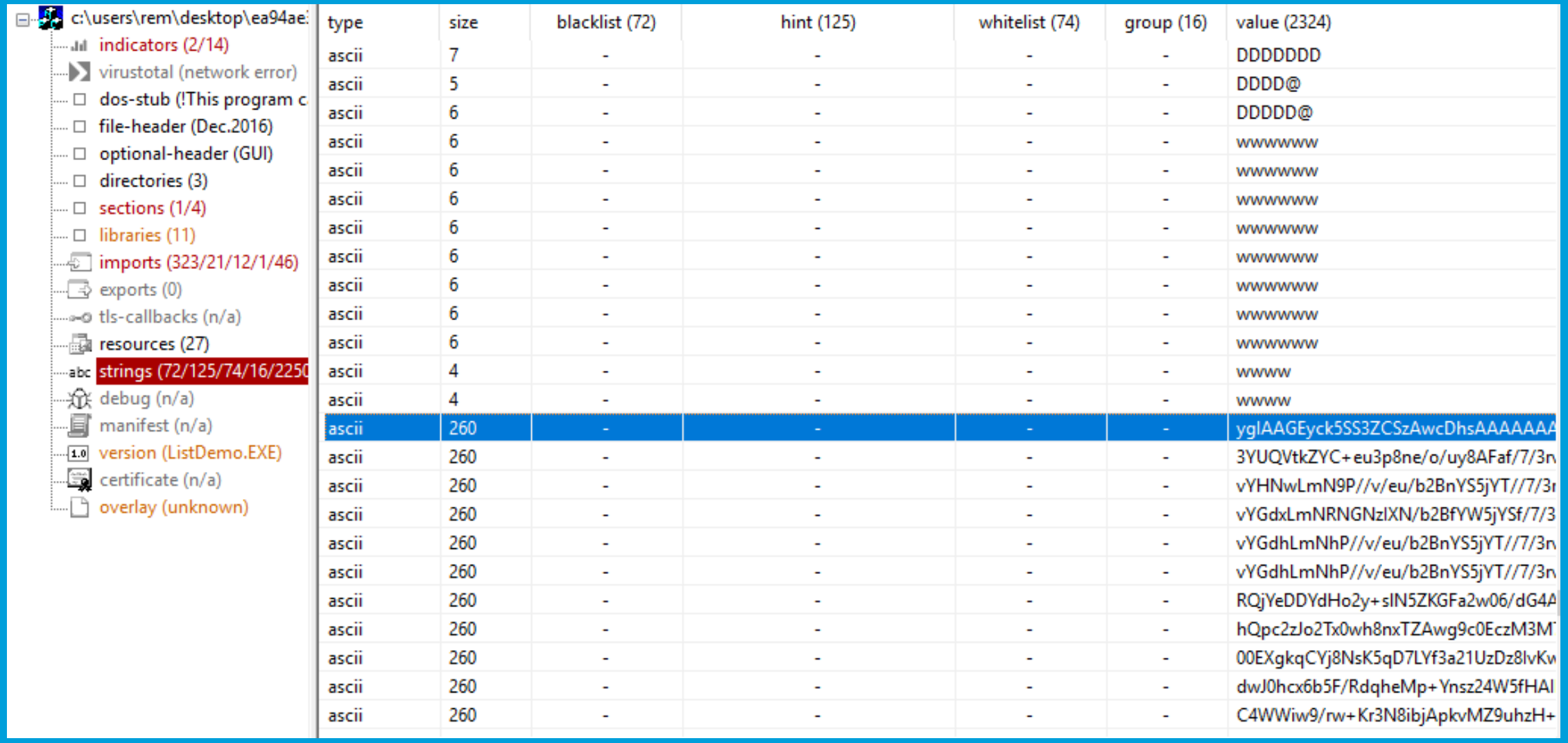
- Around Labor Day, nothing going on, needed to practice
- Was made aware of a couple of samples with new (to me) packer
- Several of us decided to look at it independently (nothing like a little competition within the team)

Preliminary exam



property	value	value	value	value
name	.text	.data	.rsrc	.pe
md5	16C9A29AB30EF2AD9AE...	10F38FF0E305E57DE96C...	006125F2F74F32DA0E89...	960048F966B32D926FB5...
file-ratio (95.94 %)	44.59 %	25.67 %	5.41 %	20.27 %
virtual-size (299764 bytes)	135168 bytes	94208 bytes	12944 bytes	57444 bytes
virtual-address	0x00001000	0x00022000	0x00039000	0x0003D000
raw-size (290816 bytes)	135168 bytes	77824 bytes	16384 bytes	61440 bytes
raw-address	0x00001000	0x00022000	0x00035000	0x00039000
cave (7436 bytes)	0 bytes	0 bytes	3440 bytes	3996 bytes
entropy	6.608	6.181	3.344	3.594
entry-point (0x0000A399)	x	-	-	-
blacklisted	-	-	-	x
writable	-	x	-	x
executable	x	-	-	-
shareable	-	-	-	-
discardable	-	-	-	-
cachable	x	x	x	x
pageable	x	x	x	x
initialized-data	-	x	x	-
uninitialized-data	-	-	-	-
readable	x	x	x	x

Preliminary exam, cont'd



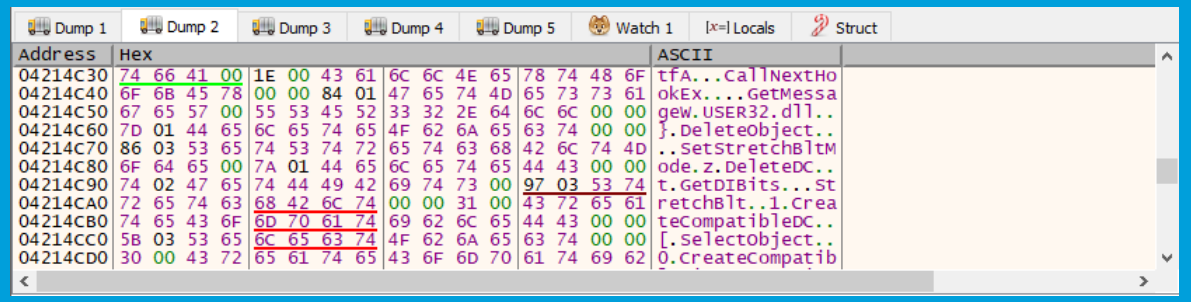
type	size	blacklist (72)	hint (125)	whitelist (74)	group (16)	value (2324)
ascii	7	-	-	-	-	DDDDDDD
ascii	5	-	-	-	-	DDDD@
ascii	6	-	-	-	-	DDDDD@
ascii	6	-	-	-	-	wwwwww
ascii	6	-	-	-	-	wwwwww
ascii	6	-	-	-	-	wwwwww
ascii	6	-	-	-	-	wwwwww
ascii	6	-	-	-	-	wwwwww
ascii	6	-	-	-	-	wwwwww
ascii	6	-	-	-	-	wwwwww
ascii	6	-	-	-	-	wwwwww
ascii	4	-	-	-	-	wwww
ascii	4	-	-	-	-	wwww
ascii	260	-	-	-	-	yglAAGEyck5SS3ZCSzAwcDhsAAAAAAA
ascii	260	-	-	-	-	3YUQVtkZYC+eu3p8ne/o/uy8AFaf/7/3n
ascii	260	-	-	-	-	vYHNwLmN9P//v/eu/b2BnYS5jYT//7/3r
ascii	260	-	-	-	-	vYGdxLmNRNGNzlXN/b2BfYW5jYSf/7/3
ascii	260	-	-	-	-	vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3n
ascii	260	-	-	-	-	vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3n
ascii	260	-	-	-	-	RQjYeDDYdHo2y+sIN5ZKGFa2w06/dG4A
ascii	260	-	-	-	-	hQpc2zJo2Tx0wh8nxTZAwg9c0EczM3M
ascii	260	-	-	-	-	00EXgkqCYj8NsK5qD7LYf3a21UzDz8lvKv
ascii	260	-	-	-	-	dwJ0hcx6b5F/RdqheMp+Ynsz24W5fHAI
ascii	260	-	-	-	-	C4WWiw9/rw+Kr3N8ibjApkvMZ9uhzH+

AT&T

Static Code Analysis

- ListDemo.exe – code example
  - Extraneous functions
- Garbage code in actual unpacking routines
- Obviously obfuscated to make analysis difficult
- Moving on…

Unpack with the debugger



- Single-step
- Breakpoints on LoadLibraryA and GetProcAddress
- Try to find the jump to OEP

Try to dump it

Fail!!!

Regroup

c:\users\rem\desktop\ea94ae:
- indicators (2/14)
- virustotal (network error)
- dos-stub (!This program c
- file-header (Dec.2016)
- optional-header (GUI)
- directories (3)
- sections (1/4)
- libraries (11)
- imports (323/21/12/1/46)
- exports (0)
- tls-callbacks (n/a)
- resources (27)
- strings (72/125/74/16/225(
- debug (n/a)
- manifest (n/a)
- version (ListDemo.EXE)
- certificate (n/a)
- overlay (unknown)

property	value	value	value	value
name	.text	.data	.rsrc	.pe
md5	16C9A29AB30EF2AD9AE...	10F38FF0E305E57DE96C...	006125F2F74F32DA0E89...	960048F966B32D926FB5...
file-ratio (95.94 %)	44.59 %	25.67 %	5.41 %	20.27 %
virtual-size (299764 bytes)	135168 bytes	94208 bytes	12944 bytes	57444 bytes
virtual-address	0x00001000	0x00022000	0x00039000	0x0003D000
raw-size (290816 bytes)	135168 bytes	77824 bytes	16384 bytes	61440 bytes
raw-address	0x00001000	0x00022000	0x00035000	0x00039000
cave (7436 bytes)	0 bytes	0 bytes	3440 bytes	3996 bytes
entropy	6.608	6.181	3.344	3.594
entry-point (0x0000A399)	x	-	-	-
blacklisted	-	-	-	x
writable	-	x	-	x
executable	x	-	-	-
shareable	-	-	-	-
discardable	-	-	-	-
cachable	x	x	x	x
pageable	x	x	x	x
initialized-data	-	x	x	-
uninitialized-data	-	-	-	-
readable	x	x	x	x

HxD - [C:\Users\REM\Desktop\EA94AE3CB4C86D1369CFD99E59D34D84D239F2C8 - Copy.exe]

File Edit Search View Analysis Extras Window ?

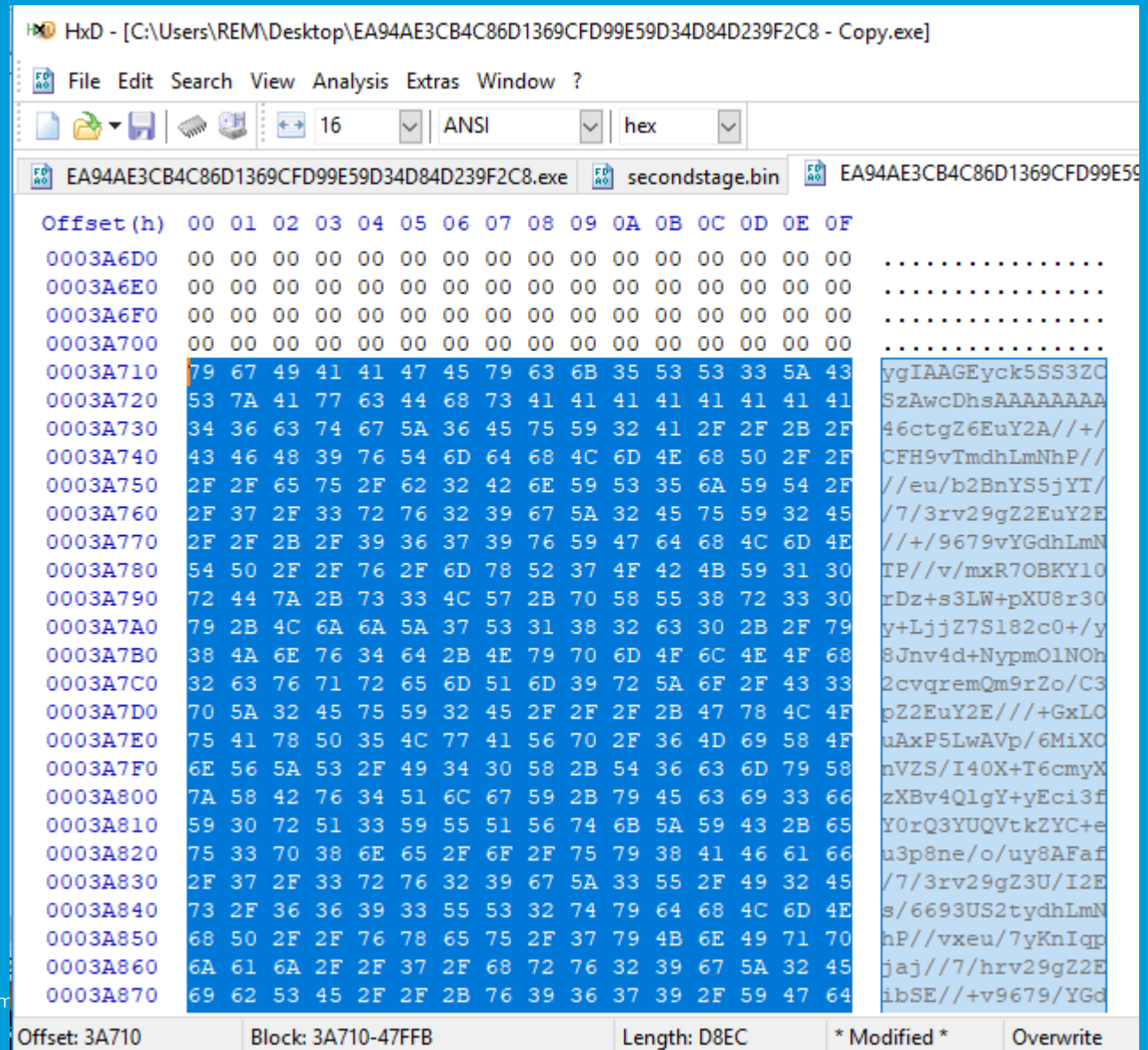
16 ANSI hex

EA94AE3CB4C86D1369CFD99E59D34D84D239F2C8.exe secondstage.bin EA94AE3CB4C86D1369CFD99E5

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00038FF0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00039000   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00039010   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00039020   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00039030   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00039040   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00039050   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00039060   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00039070   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00039080   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00039090   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000390A0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000390B0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000390C0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000390D0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000390E0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000390F0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00039100   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00039110   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00039120   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00039130   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00039140   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00039150   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00039160   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00039170   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00039180   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00039190   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

Offset: 3A710 | Block: 3A710-47FFB | Length: D8EC | * Modified * | Overwrite

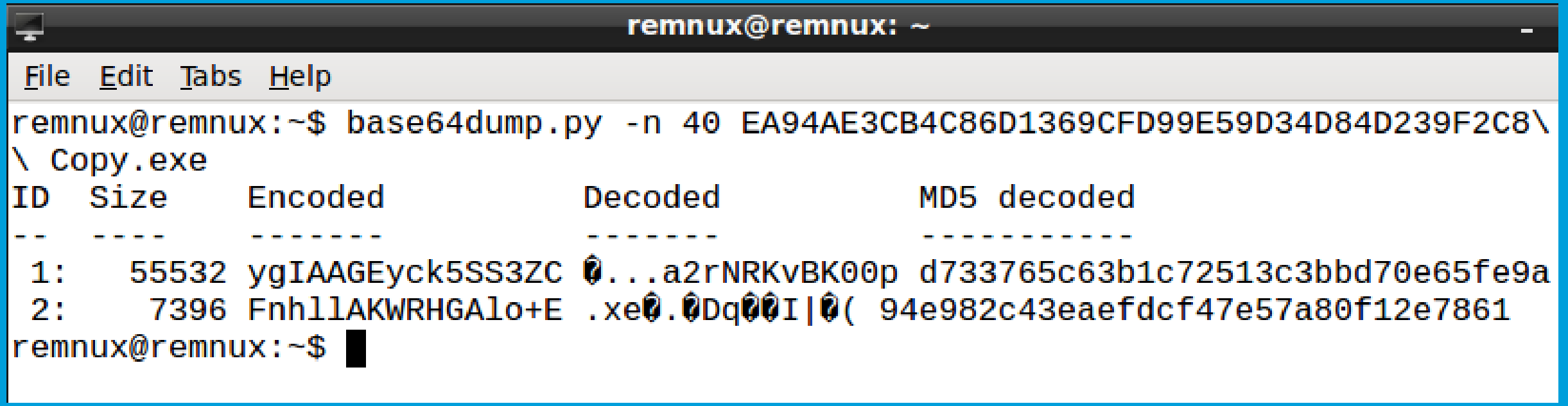
Hmm…

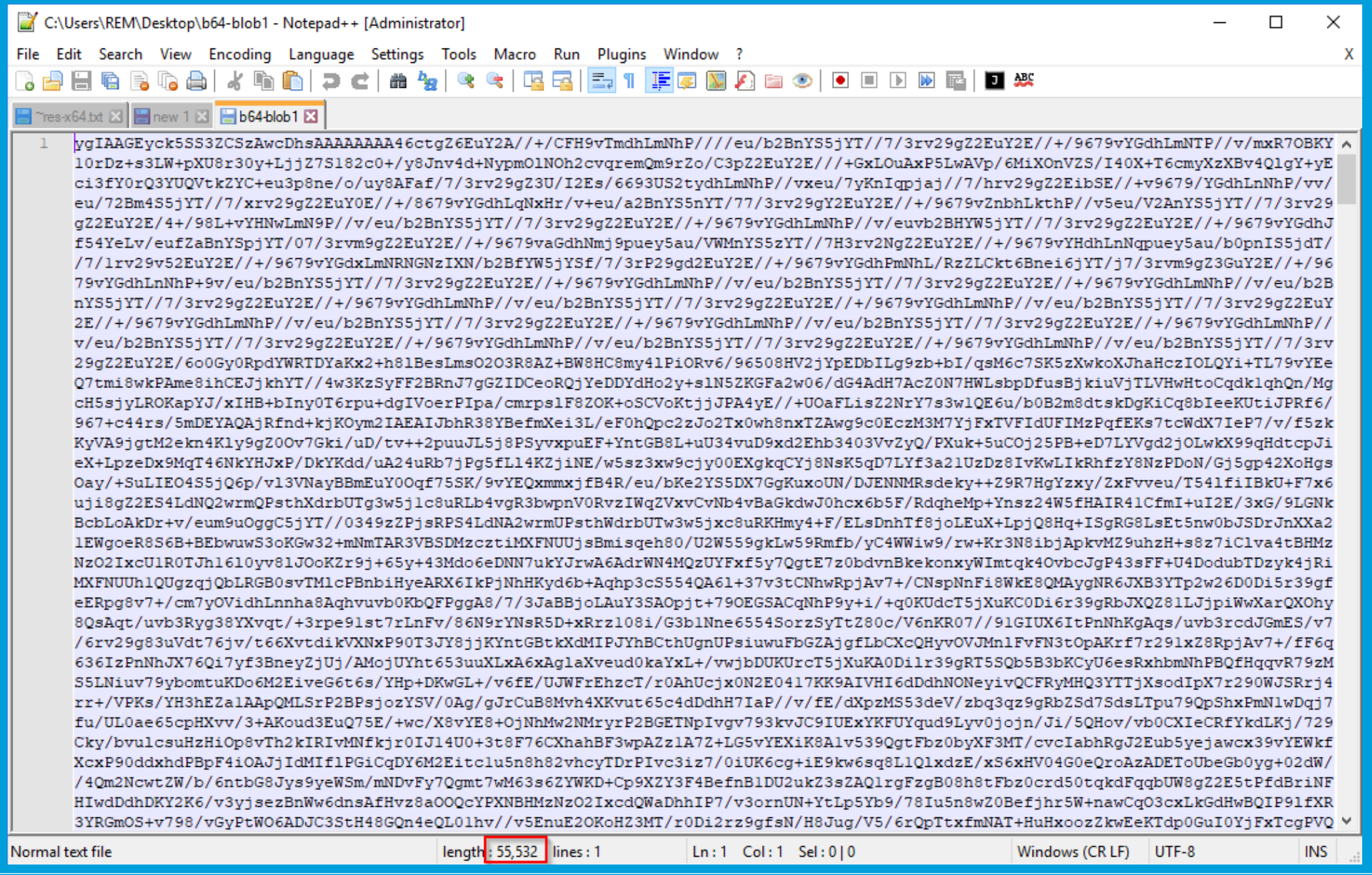


If at first, you don't succeed, try som

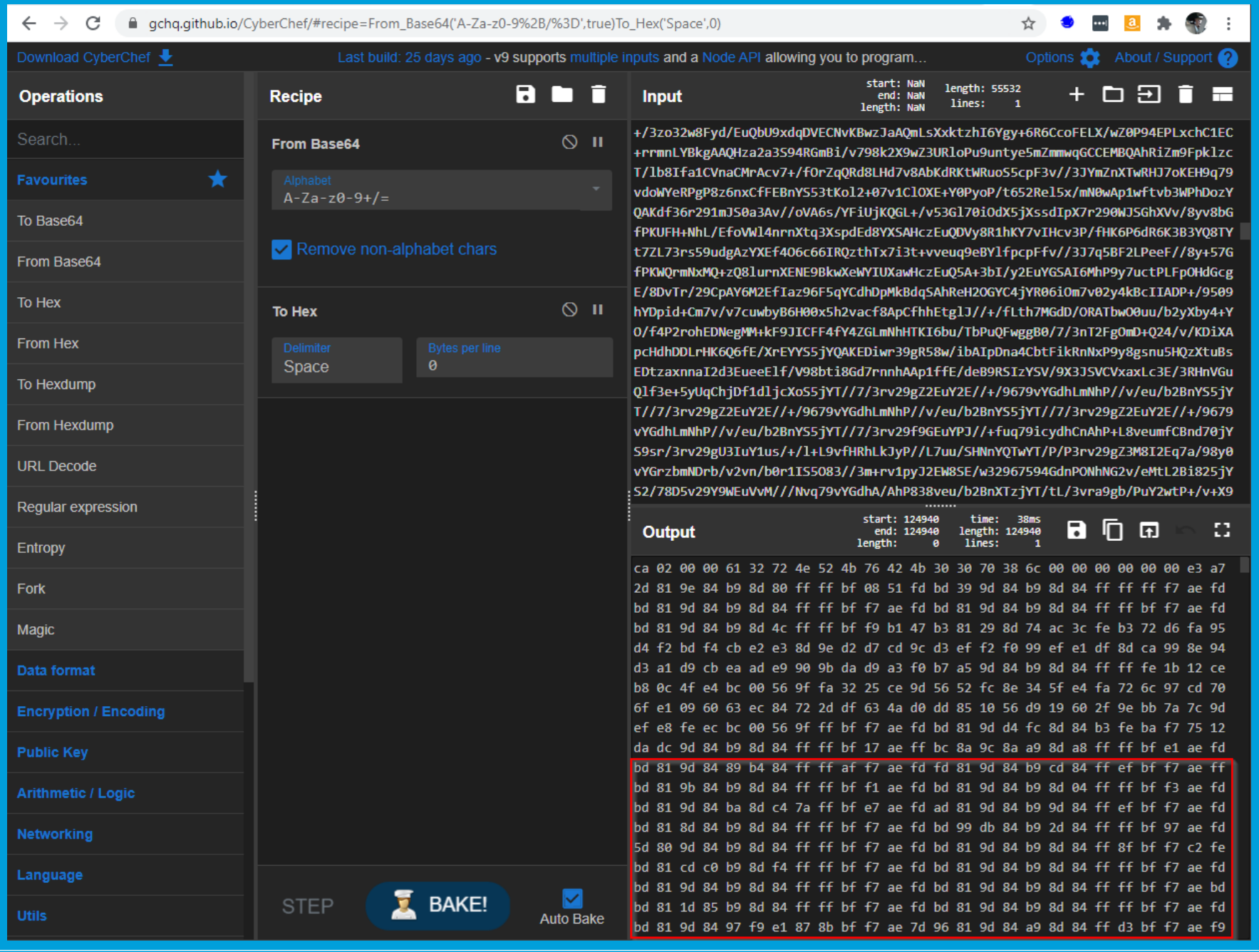
AT&T

Those base64 strings look interesting




C:\Users\REM\Desktop\b64-blob1 - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
~res-x64.txt
new 1
b64-blob1
1
ygIAAGEyck5SS3ZCSzAwcDhsAAAAAAAA46ctgZ6EuY2A//+/CFH9vTmdhLmNhP////eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNTP//v/mxR7OBKY
l0rDz+s3LW+pXU8r30y+LjjZ7Sl82c0+/y8Jnv4d+NypmOlNOh2cvqremQm9rZo/C3pZ2EuY2E///+GxLOuAxP5LwAVp/6MiXOnVZS/I40X+T6cmyXzXBv4QlgY+yE
ci3fY0rQ3YUQVtkZYC+eu3p8ne/o/uy8AFaf/7/3rv29gZ3U/I2Es/6693US2tydhLmNhP//vxeu/7yKnIqpjaj//7/hrv29gZ2EibSE//+v9679/YGdhLnNhP/vv/
eu/72Bm4S5jYT//7/xrv29gZ2EuY0E//+/8679vYGdhLqNxHr/v+eu/a2BnYS5nYT/77/3rv29gY2EuY2E//+/9679vZnbhLkthP//v5eu/V2AnYS5jYT//7/3rv29
gZ2EuY2E/4+/98L+vYHNwLmN9P//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/euvb2BHYW5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhJ
f54YeLv/eufZaBnYSpjYT/07/3rvm9gZ2EuY2E//+/9679vaGdhNmj9puey5au/VWMnYS5zYT//7H3rv2NgZ2EuY2E//+/9679vYHdhLnNqpuey5au/b0pnIS5jdT/
//7/lrv29v52EuY2E//+/9679vYGdxLmNRNGNzIXN/b2BfYW5jYSf/7/3rP29gd2EuY2E//+/9679vYGdhPmNhL/RzZLCkt6Bnei6jYT/j7/3rvm9gZ3GuY2E//+/96
79vYGdhLnNhP+9v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2B
nYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY
2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//
v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv
29gZ2EuY2E/6o0Gy0RpdYWRTDYaKx2+h81BesLmsO2O3R8AZ+BW8HC8my4lPiORv6/96508HV2jYpEDbILg9zb+bI/qsM6c7SK5zXwkoXJhaHczIOLQYi+TL79vYEe
Q7tmi8wkPAme8ihCEJjkhYT//4w3KzSyFF2BRnJ7gGZIDCeoRQjYeDDYdHo2y+slN5ZKGFa2w06/dG4AdH7AcZ0N7HWLsbpDfusBjkiuVjTLVHwHtoCqdklqhQn/Mg
cH5sjyLROKapYJ/xIHB+bIny0T6rpu+dgIVoerPIpa/cmrpslF8ZOK+oSCVoKtjjJPA4yE//+UOaFLisZ2NrY7s3wlQE6u/b0B2m8dtskDgKiCq8bIeeKUtiJPRf6/
967+c44rs/5mDEYAQAjRfnd+kjKOym2IAEAIJbhR38YBefmXei3L/eF0hQpc2zJo2Tx0wh8nxTZAwg9c0EczM3M7YjFxTVFIdUFIMzPqfEKs7tcWdX7IeP7/v/f5zk
KyVA9jgtM2ekn4Kly9gZ0Ov7Gki/uD/tv++2puuJL5j8PSyvxpuEF+YntGB8L+uU34vuD9xd2Ehb3403VvZyQ/PXuk+5uCOj25PB+eD7LYVgd2jOLwkX99qHdtcpJi
eX+LpzeDx9MqT46NkYHJxP/DkYKdd/uA24uRb7jPg5fLl4KZjiNE/w5sz3xw9cjy00EXgkqCYj8NsK5qD7LYf3a21UzDz8IvKwLIkRhfzY8NzPDoN/Gj5gp42XoHgs
Oay/+SuLIEO4S5jQ6p/vl3VNayBBmEuY0Oqf75SK/9vYEQxmmxjfB4R/eu/bKe2YS5DX7GgKuxoUN/DJENNMRsdeky++Z9R7HgYzxy/ZxFvveu/T54lfiIBkU+F7x6
uji8gZ2ES4LdNQ2wrmQPsthXdrbUTg3w5j1c8uRLb4vgR3bwpnV0RvzIWqZVxvCvNb4vBaGkdwJ0hcx6b5F/RdqheMp+Ynsz24W5fHAIR41CfmI+uI2E/3xG/9LGNk
BcbLoAkDr+v/eum9uOggC5jYT//0349zZPjsRPS4LdNA2wrmUPsthWdrbUTw3w5jxc8uRKHmy4+F/ELsDnhTf8joLEuX+LpjQ8Hq+ISgRG8LsEt5nw0bJSDrJnXXa2
lEWgoeR8S6B+BEbwuwS3oKGw32+mNmTAR3VBSDMzcztiMXFNUUjsBmisqeh80/U2W559gkLw59Rmfb/yC4WWiw9/rw+Kr3N8ibjApkvMZ9uhzH+s8z7iClva4tBHMz
NzO2IxcUlR0TJhl6l0yv8lJOoKZr9j+65y+43Mdo6eDNN7ukYJrwA6AdrWN4MQzUYFxf5y7QgtE7z0bdvnBkekonxyWImtqk4OvbcJgP43sFF+U4DodubTDzyk4jRi
MXFNUUhlQUgzqjQbLRGB0svTMlcPBnbiHyeARX6IkPjNhHKyd6b+Aqhp3cS554QA6l+37v3tCNhwRpjAv7+/CNspNnFi8WkE8QMAygNR6JXB3YTp2w26D0Di5r39gf
eERpg8v7+/cm7yOVidhLnnha8Aqhvuvb0KbQFPggA8/7/3JaBBjoLAuY3SAOpjt+79OEGSACqNhP9y+i/+q0KUdcT5jXuKC0Di6r39gRbJXQZ8lLJjpiWwXarQXOhy
8QsAqt/uvb3Ryg38YXvqt/+3rpe9lst7rLnFv/86N9rYNsR5D+xRrzl08i/G3blNne6554SorzSyTtZ80c/V6nKR07//9lGIUX6ItPnNhKgAqs/uvb3rcdJGmES/v7
/6rv29g83uVdt76jv/t66XvtdikVXNxP90T3JY8jjKYntGBtkXdMIPJYhBCthUgnUPsiuwuFbGZAjgfLbCXcQHyvOVJMnlFvFN3tOpAKrf7r291xZ8RpjAv7+/fF6q
636IzPnNhJX76Qi7yf3BneyZjUj/AMojUYht653uuXLxA6xAglaXveud0kaYxL+/vwjbDUKUrcT5jXuKA0Dilr39gRT5SQb5B3bKCyU6esRxhbmNhPBQfHqqvR79zM
S5LNiuv79ybomtuKDo6M2EiveG6t6s/YHp+DKwGL+/v6fE/UJWFrEhzcT/r0AhUcjx0N2E0417KK9AIVHI6dDdhNONeyivQCFRyMHQ3YTTjXsodIpX7r290WJSRrj4
rr+/VPKs/YH3hEZalAApQMLSrP2BPsjozYSV/0Ag/gJrCuB8Mvh4XKvut65c4dDdhH7IaP//v/fE/dXpzMS53deV/zbq3qz9gRbZSd7SdsLTpu79QpShxPmNlwDqj7
fu/UL0ae65cpHXvv/3+AKoud3EuQ75E/+wc/X8vYE8+OjNhMw2NMryrP2BGETNpIvgv793kvJC9IUExYKFUYqud9Lyv0jojn/Ji/5QHov/vb0CXIeCRfYkdLKj/729
Cky/bvulcsuHzHiOp8vTh2kIRIvMNfkjr0IJ14U0+3t8F76CXhahBF3wpAZzlA7Z+LG5vYEXiK8Alv539QgtFbz0byXF3MT/cvcIabhRgJ2Eub5yejawcx39vYEWkf
XcxP90ddxhdPBpF4iOAJjIdMIflPGiCqDY6M2Eitclu5n8h82vhcyTDrPIvc3iz7/0iUK6cg+iE9kw6sq8LlQlxdzE/xS6xHV04G0eQroAzADEToUbeGb0yg+02dW/
/4Qm2NcwtZW/b/6ntbG8Jys9yeWSm/mNDvFy7Qgmt7wM63s6ZYWKD+Cp9XZY3F4BefnBlDU2ukZ3sZAQlrgFzgB08h8tFbz0crd50tqkdFqqbUW8gZ2E5tPfdBriNF
HIwdDdhDKY2K6/v3yjsezBnWw6dnsAfHvz8aOOQcYPXNBHMzNzO2IxcdQWaDhhIP7/v3ornUN+YtLp5Yb9/78Iu5n8wZ0Befjhr5W+nawCqO3cxLkGdHwBQIP91fXR
3YRGmOS+v798/vGyPtWO6ADJC3StH48GQn4eQL0lhv//v5EnuE2OKoHZ3MT/r0Di2rz9gfsN/H8Jug/V5/6rQpTtxfmNAT+HuHxoozZkwEeKTdp0GuI0YjFxTcgPVQ
Normal text file
length : 55,532
lines : 1
Ln : 1 Col : 1 Sel : 0 | 0
Windows (CR LF)
UTF-8
INS

AT&T

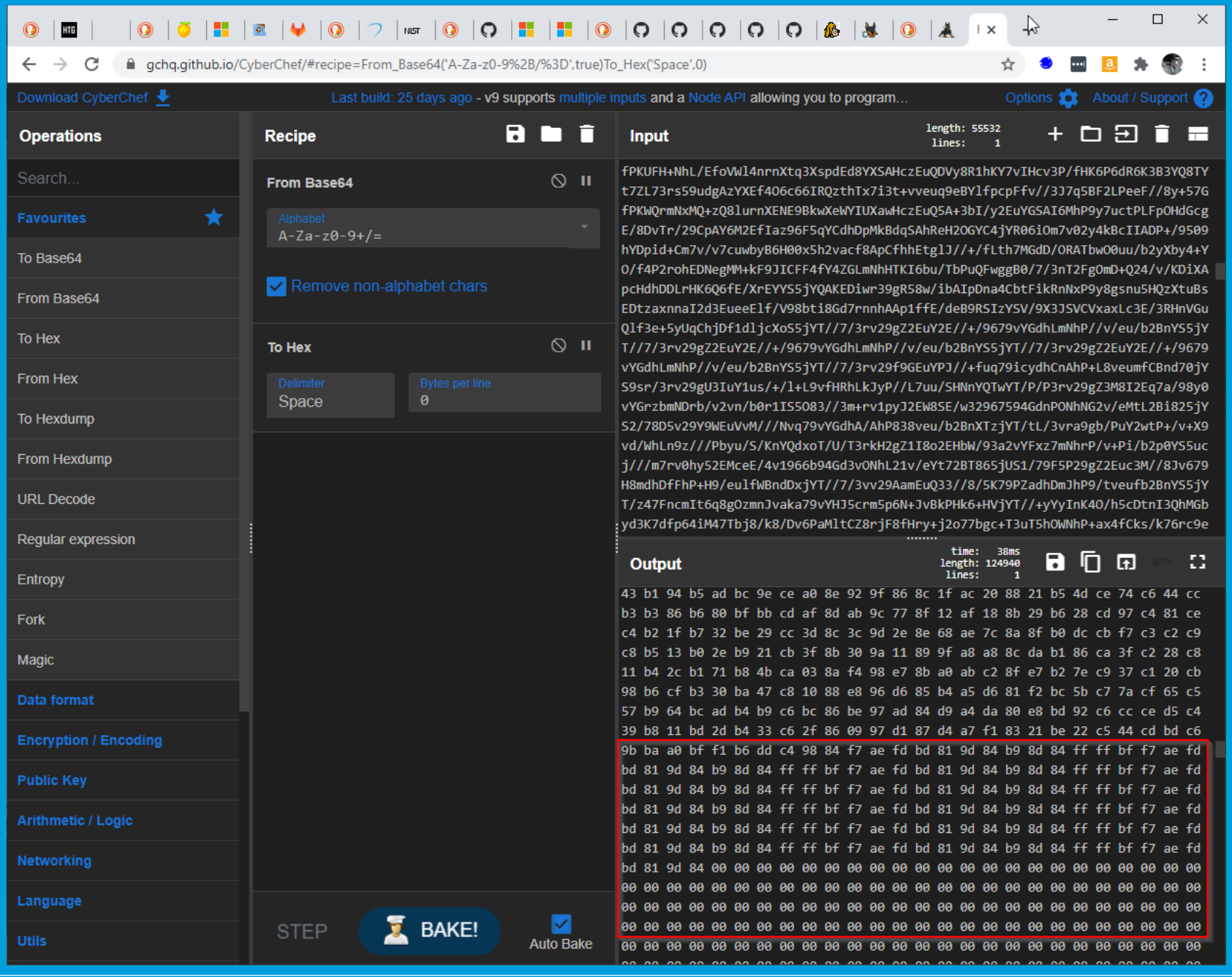

gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true)To_Hex('Space',0)
Download CyberChef
Last build: 25 days ago - v9 supports multiple inputs and a Node API allowing you to program...
Options
About / Support
Operations
Search...
Favourites
To Base64
From Base64
To Hex
From Hex
To Hexdump
From Hexdump
URL Decode
Regular expression
Entropy
Fork
Magic
Data format
Encryption / Encoding
Public Key
Arithmetic / Logic
Networking
Language
Utils
Recipe
From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars
To Hex
Delimiter
Space
Bytes per line
0
STEP
BAKE!
Auto Bake
Input
start: NaN
end: NaN
length: NaN
length: 55532
lines: 1
+/3zo32w8Fyd/EuQbU9xdqDVECNvKBwzJaAQmLsXxktzhI6Ygy+6R6CcoFELX/wZ0P94EPLxchC1EC
+rrmnLYBkgAAQHza2a3S94RGmBi/v798k2X9wZ3URloPu9untye5mZmmwqGCCEMBQAhRiZm9Fpklzc
T/lb8Ifa1CVnaCMrAcv7+/fOrZqQRd8LHd7v8AbKdRKtWRuoS5cpF3v//3JYmZnXTwRHJ7oKEH9q79
vdoWYeRPgP8z6nxCfFEBnYS53tKol2+07v1ClOXE+Y0PyoP/t652Rel5x/mN0wAp1wftvb3WPhDozY
QAKdf36r291mJS0a3Av//oVA6s/YFiUjKQGL+/v53Gl70iOdX5jXssdIpX7r290WJSGhXVv/8yv8bG
fPKUFH+NhL/EfoVWl4nrnXtq3XspdEd8YXSAHczEuQDVy8R1hKY7vIHcv3P/fHK6P6dR6K3B3YQ8TY
t7ZL73rs59udgAzYXEf4O6c66IRQzthTx7i3t+vveuq9eBYlfpcpFfv//3J7q5BF2LPeeF//8y+57G
fPKWQrmNxMQ+zQ8lurnXENE9BkwXeWYIUXawHczEuQ5A+3bI/y2EuYGSAI6MhP9y7uctPLFpOHdGcg
E/8DvTr/29CpAY6M2EfIaz96F5qYCdhDpMkBdqSAhReH2OGYC4jYR06iOm7v02y4kBcIIADP+/9509
hYDpid+Cm7v/v7cuwbyB6H00x5h2vacf8ApCfhhEtglJ//+/fLth7MGdD/ORATbwO0uu/b2yXby4+Y
O/f4P2rohEDNegMM+kF9JICFF4fY4ZGLmNhHTKI6bu/TbPuQFwggB0/7/3nT2FgOmD+Q24/v/KDiXA
pcHdhDDLrHK6Q6fE/XrEYYS5jYQAKEDiwr39gR58w/ibAIpDna4CbtFikRnNxP9y8gsnu5HQzXtuBs
EDtzaxnnaI2d3EueeElf/V98bti8Gd7rnnhAAp1ffE/deB9RSIzYSV/9X3JSVCVxaxLc3E/3RHnVGu
Qlf3e+5yUqChjDf1dljcXoS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jY
T//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679
vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29f9GEuYPJ//+fuq79icydhCnAhP+L8veumfCBnd70jY
S9sr/3rv29gU3IuY1us/+/l+L9vfHRhLkJyP//L7uu/SHNnYQTwYT/P/P3rv29gZ3M8I2Eq7a/98y0
vYGrzbmNDrb/v2vn/b0r1IS5O83//3m+rv1pyJ2EW8SE/w32967594GdnPONhNG2v/eMtL2Bi825jY
S2/78D5v29Y9WEuVvM///Nvq79vYGdhA/AhP838veu/b2BnXTzjYT/tL/3vra9gb/PuY2wtP+/v+X9

Output
start: 124940
end: 124940
length: 0
time: 38ms
length: 124940
lines: 1
ca 02 00 00 61 32 72 4e 52 4b 76 42 4b 30 30 70 38 6c 00 00 00 00 00 00 e3 a7
2d 81 9e 84 b9 8d 80 ff ff bf 08 51 fd bd 39 9d 84 b9 8d 84 ff ff ff f7 ae fd
bd 81 9d 84 b9 8d 84 ff ff bf f7 ae fd bd 81 9d 84 b9 8d 84 ff ff bf f7 ae fd
bd 81 9d 84 b9 8d 4c ff ff bf f9 b1 47 b3 81 29 8d 74 ac 3c fe b3 72 d6 fa 95
d4 f2 bd f4 cb e2 e3 8d 9e d2 d7 cd 9c d3 ef f2 f0 99 ef e1 df 8d ca 99 8e 94
d3 a1 d9 cb ea ad e9 90 9b da d9 a3 f0 b7 a5 9d 84 b9 8d 84 ff ff fe 1b 12 ce
b8 0c 4f e4 bc 00 56 9f fa 32 25 ce 9d 56 52 fc 8e 34 5f e4 fa 72 6c 97 cd 70
6f e1 09 60 63 ec 84 72 2d df 63 4a d0 dd 85 10 56 d9 19 60 2f 9e bb 7a 7c 9d
ef e8 fe ec bc 00 56 9f ff bf f7 ae fd bd 81 9d d4 fc 8d 84 b3 fe ba f7 75 12
da dc 9d 84 b9 8d 84 ff ff bf 17 ae ff bc 8a 9c 8a a9 8d a8 ff ff bf e1 ae fd
bd 81 9d 84 89 b4 84 ff ff af f7 ae fd fd 81 9d 84 b9 cd 84 ff ef bf f7 ae ff
bd 81 9b 84 b9 8d 84 ff ff bf f1 ae fd bd 81 9d 84 b9 8d 04 ff ff bf f3 ae fd
bd 81 9d 84 ba 8d c4 7a ff bf e7 ae fd ad 81 9d 84 b9 9d 84 ff ef bf f7 ae fd
bd 81 8d 84 b9 8d 84 ff ff bf f7 ae fd bd 99 db 84 b9 2d 84 ff ff bf 97 ae fd
5d 80 9d 84 b9 8d 84 ff ff bf f7 ae fd bd 81 9d 84 b9 8d 84 ff 8f bf f7 c2 fe
bd 81 cd c0 b9 8d f4 ff ff bf f7 ae fd bd 81 9d 84 b9 8d 84 ff ff bf f7 ae fd
bd 81 9d 84 b9 8d 84 ff ff bf f7 ae fd bd 81 9d 84 b9 8d 84 ff ff bf f7 ae bd
bd 81 1d 85 b9 8d 84 ff ff bf f7 ae fd bd 81 9d 84 b9 8d 84 ff ff bf f7 ae fd
bd 81 9d 84 97 f9 e1 87 8b bf f7 ae 7d 96 81 9d 84 a9 8d 84 ff d3 bf f7 ae f9

AT&T

Lots of repetition, could there be a key in there

```
bd 81 9d 84 89 b4 84 ff ff af f7 ae fd fd 81 9d 84 b9 cd 84 ff ef bf f7 ae ff
bd 81 9b 84 b9 8d 84 ff ff bf f1 ae fd bd 81 9d 84 b9 8d 04 ff ff bf f3 ae fd
bd 81 9d 84 ba 8d c4 7a ff bf e7 ae fd ad 81 9d 84 b9 9d 84 ff ef bf f7 ae fd
bd 81 8d 84 b9 8d 84 ff ff bf f7 ae fd bd 99 db 84 b9 2d 84 ff ff bf 97 ae fd
5d 80 9d 84 b9 8d 84 ff ff bf f7 ae fd bd 81 9d 84 b9 8d 84 ff 8f bf f7 c2 fe
bd 81 cd c0 b9 8d f4 ff ff bf f7 ae fd bd 81 9d 84 b9 8d 84 ff ff bf f7 ae fd
bd 81 9d 84 b9 8d 84 ff ff bf f7 ae fd bd 81 9d 84 b9 8d 84 ff ff bf f7 ae bd
bd 81 1d 85 b9 8d 84 ff ff bf f7 ae fd bd 81 9d 84 b9 8d 84 ff ff bf f7 ae fd
bd 81 9d 84 97 f9 e1 87 8b bf f7 ae 7d 96 81 9d 84 a9 8d 84 ff d3 bf f7 ae f9
```

gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true)To_Hex('Space',0)

From Base64

Alphabet: A-Za-z0-9+/=

☑ Remove non-alphabet chars

To Hex

Delimiter: Space

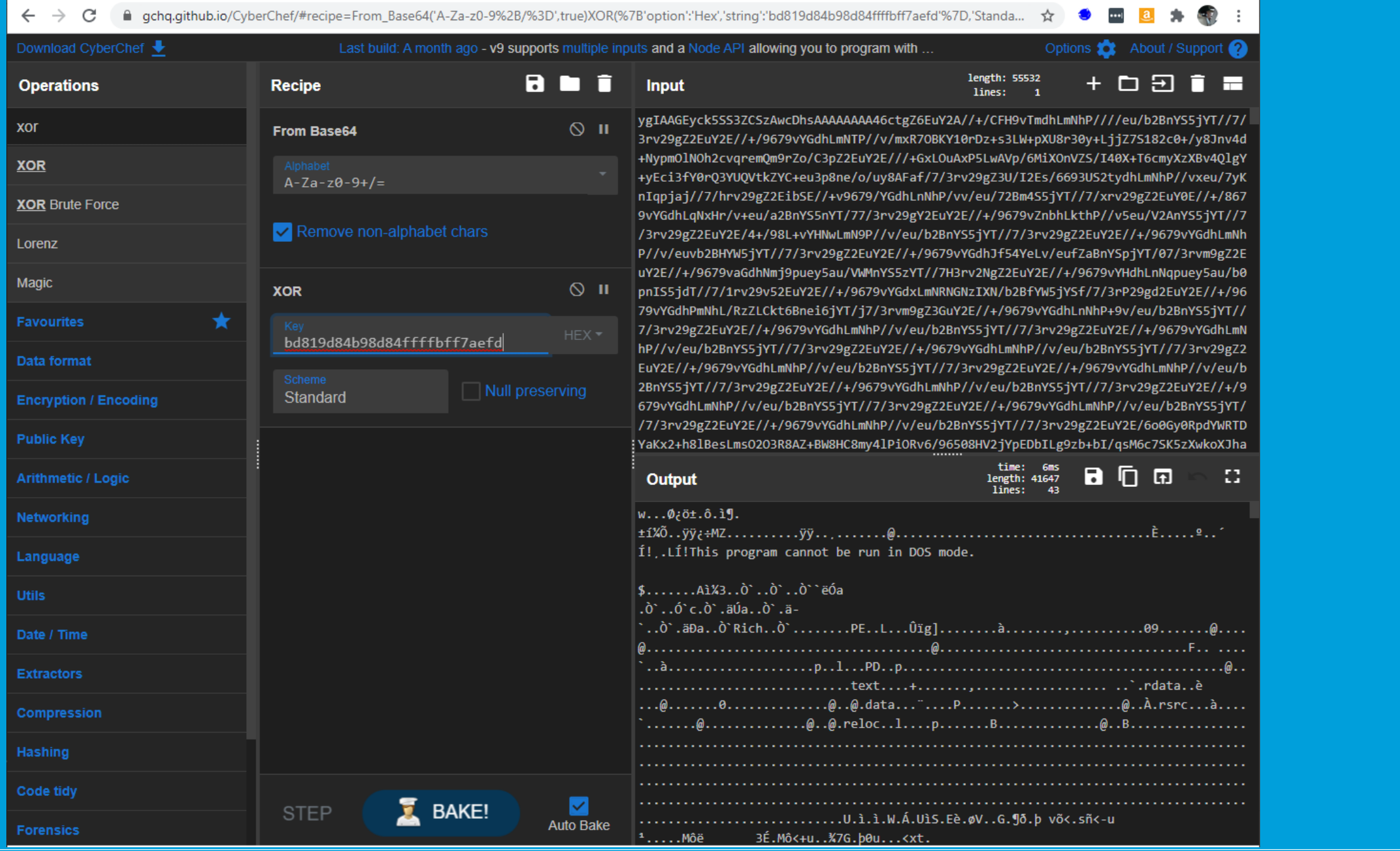
Bytes per line: 0

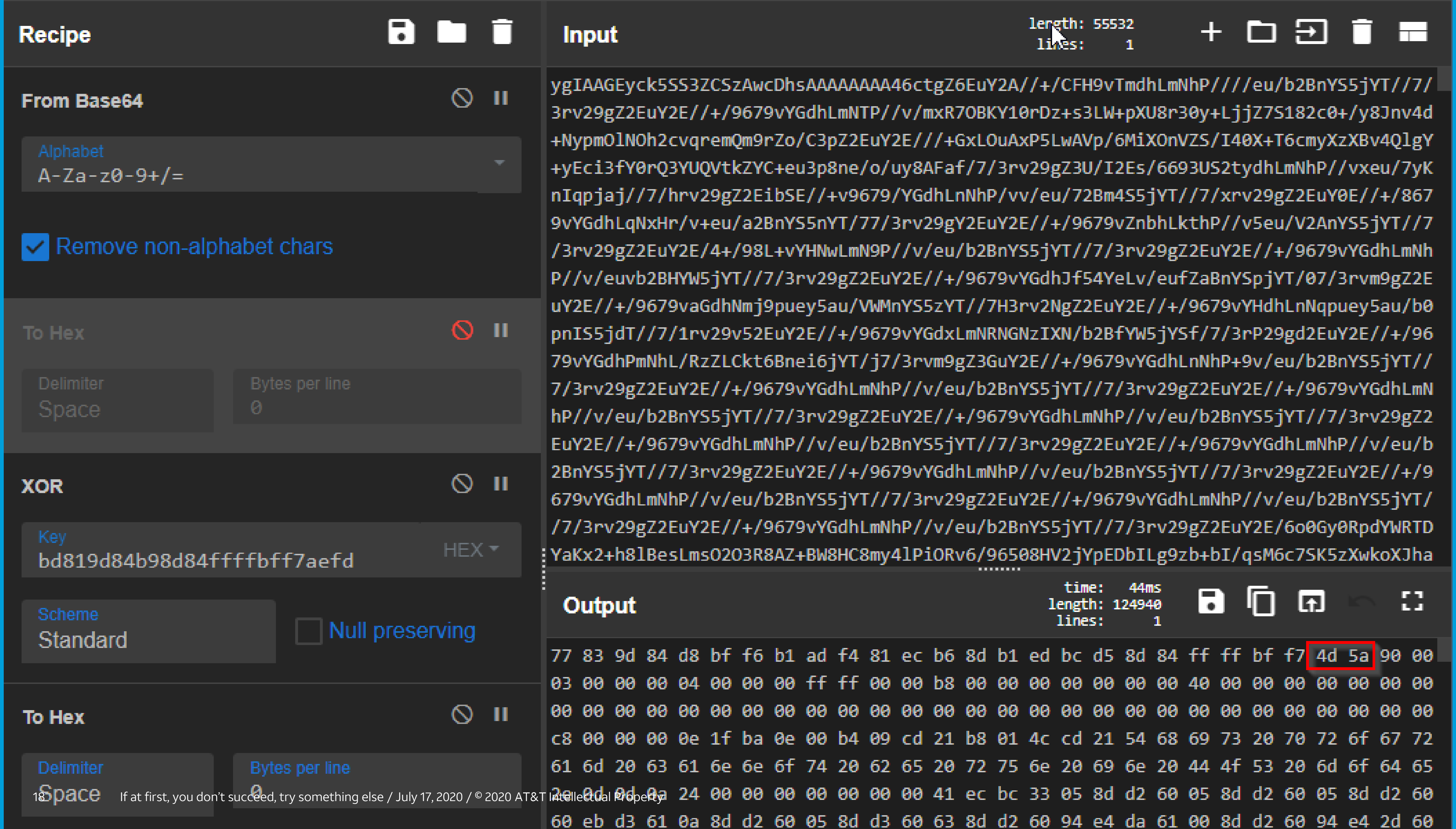
```
length: 55532
 lines:     1
```

```
fPKUFH+NhL/EfoVWl4nrnXtq3XspdEd8YXSAHczEuQDVy8R1hKY7vIHcv3P/fHK6P6dR6K3B3YQ8TY
t7ZL73rs59udgAzYXEf4O6c66IRQzthTx7i3t+vveuq9eBYlfpcpFfv//3J7q5BF2LPeeF//8y+57G
fPKWQrmNxMQ+zQ8lurnXENE9BkwXeWYIUXawHczEuQ5A+3bI/y2EuYGSAI6MhP9y7uctPLFpOHdGcg
E/8DvTr/29CpAY6M2EfIaz96F5qYCdhDpMkBdqSAhReH2OGYC4jYR06iOm7v02y4kBcIIADP+/9509
hYDpid+Cm7v/v7cuwbyB6H00x5h2vacf8ApCfhhEtglJ//+/fLth7MGdD/ORATbwO0uu/b2yXby4+Y
O/f4P2rohEDNegMM+kF9JICFF4fY4ZGLmNhHTKI6bu/TbPuQFwggB0/7/3nT2FgOmD+Q24/v/KDiXA
pcHdhDDLrHK6Q6fE/XrEYYS5jYQAKEDiwr39gR58w/ibAIpDna4CbtFikRnNxP9y8gsnu5HQzXtuBs
EDtzaxnnaI2d3EueeElf/V98bti8Gd7rnnhAAp1ffE/deB9RSIzYSV/9X3JSVCVxaxLc3E/3RHnVGu
Qlf3e+5yUqChjDf1dljcXoS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jY
T//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679
vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29f9GEuYPJ//+fuq79icydhCnAhP+L8veumfCBnd70jY
S9sr/3rv29gU3IuY1us/+/l+L9vfHRhLkJyP//L7uu/SHNnYQTwYT/P/P3rv29gZ3M8I2Eq7a/98y0
vYGrzbmNDrb/v2vn/b0r1IS5O83//3m+rv1pyJ2EW8SE/w32967594GdnPONhNG2v/eMtL2Bi825jY
S2/78D5v29Y9WEuVvM///Nvq79vYGdhA/AhP838veu/b2BnXTzjYT/tL/3vra9gb/PuY2wtP+/v+X9
vd/WhLn9z///Pbyu/S/KnYQdxoT/U/T3rkH2gZ1I8o2EHbW/93a2vYFxz7mNhrP/v+Pi/b2p0YS5uc
j///m7rv0hy52EMceE/4v1966b94Gd3vONhL21v/eYt72BT865jUS1/79F5P29gZ2Euc3M//8Jv679
H8mdhDfFhP+H9/eulfWBndDxjYT//7/3vv29AamEuQ33//8/5K79PZadhDmJhP9/tveufb2BnYS5jY
T/z47FncmIt6q8gOzmnJvaka79vYHJ5crm5p6N+JvBkPHk6+HVjYT//+yYyInK4O/h5cDtnI3QhMGb
yd3K7dfp64iM47Tbj8/k8/Dv6PaMltCZ8rjF8fHry+j2o77bgc+T3uT5hOWNhP+ax4fCks/k76rc9e
```

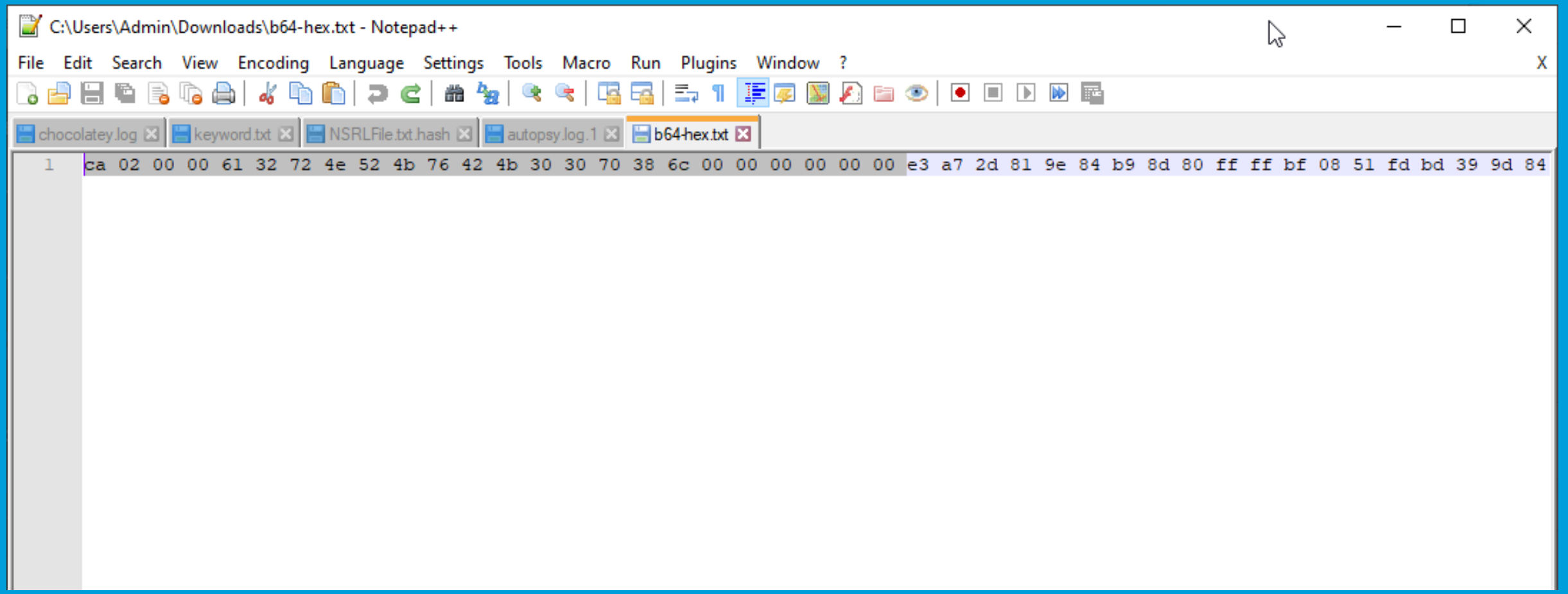
```
   time:   38ms
 length: 124940
  lines:      1
```

```
43 b1 94 b5 ad bc 9e ce a0 8e 92 9f 86 8c 1f ac 20 88 21 b5 4d ce 74 c6 44 cc
b3 b3 86 b6 80 bf bb cd af 8d ab 9c 77 8f 12 af 18 8b 29 b6 28 cd 97 c4 81 ce
c4 b2 1f b7 32 be 29 cc 3d 8c 3c 9d 2e 8e 68 ae 7c 8a 8f b0 dc cb f7 c3 c2 c9
c8 b5 13 b0 2e b9 21 cb 3f 8b 30 9a 11 89 9f a8 a8 8c da b1 86 ca 3f c2 28 c8
11 b4 2c b1 71 b8 4b ca 03 8a f4 98 e7 8b a0 ab c2 8f e7 b2 7e c9 37 c1 20 cb
98 b6 cf b3 30 ba 47 c8 10 88 e8 96 d6 85 b4 a5 d6 81 f2 bc 5b c7 7a cf 65 c5
57 b9 64 bc ad b4 b9 c6 bc 86 be 97 ad 84 d9 a4 da 80 e8 bd 92 c6 cc ce d5 c4
39 b8 11 bd 2d b4 33 c6 2f 86 09 97 d1 87 d4 a7 f1 83 21 be 22 c5 44 cd bd c6
9b ba a0 bf f1 b6 dd c4 98 84 f7 ae fd bd 81 9d 84 b9 8d 84 ff ff bf f7 ae fd
bd 81 9d 84 b9 8d 84 ff ff bf f7 ae fd bd 81 9d 84 b9 8d 84 ff ff bf f7 ae fd
bd 81 9d 84 b9 8d 84 ff ff bf f7 ae fd bd 81 9d 84 b9 8d 84 ff ff bf f7 ae fd
bd 81 9d 84 b9 8d 84 ff ff bf f7 ae fd bd 81 9d 84 b9 8d 84 ff ff bf f7 ae fd
bd 81 9d 84 b9 8d 84 ff ff bf f7 ae fd bd 81 9d 84 b9 8d 84 ff ff bf f7 ae fd
bd 81 9d 84 b9 8d 84 ff ff bf f7 ae fd bd 81 9d 84 b9 8d 84 ff ff bf f7 ae fd
bd 81 9d 84 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```


gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true)XOR(%7B'option':'Hex','string':'bd819d84b98d84ffffbff7aefd'%7D,'Standa...
Download CyberChef
Last build: A month ago - v9 supports multiple inputs and a Node API allowing you to program with ...
Options
About / Support
Operations
xor
XOR
XOR Brute Force
Lorenz
Magic
Favourites
Data format
Encryption / Encoding
Public Key
Arithmetic / Logic
Networking
Language
Utils
Date / Time
Extractors
Compression
Hashing
Code tidy
Forensics
Recipe
From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars
XOR
Key
bd819d84b98d84ffffbff7aefd
HEX
Scheme
Standard
Null preserving
STEP
BAKE!
Auto Bake
Input
length: 55532
lines: 1
ygIAAGEyck5SS3ZCSzAwcDhsAAAAAAAA46ctgZ6EuY2A//+/CFH9vTmdhLmNhP////eu/b2BnYS5jYT//7/
3rv29gZ2EuY2E//+/9679vYGdhLmNTP//v/mxR7OBKY10rDz+s3LW+pXU8r30y+LjjZ7S182c0+/y8Jnv4d
+NypmOlNOh2cvqremQm9rZo/C3pZ2EuY2E///+GxLOuAxP5LwAVp/6MiXOnVZS/I40X+T6cmyXzXBv4QlgY
+yEci3fY0rQ3YUQVtkZYC+eu3p8ne/o/uy8AFaf/7/3rv29gZ3U/I2Es/6693US2tydhLmNhP//vxeu/7yK
nIqpjaj//7/hrv29gZ2EibSE//+v9679/YGdhLnNhP/vv/eu/72Bm4S5jYT//7/xrv29gZ2EuY0E//+/867
9vYGdhLqNxHr/v+eu/a2BnYS5nYT/77/3rv29gY2EuY2E//+/9679vZnbhLkthP//v5eu/V2AnYS5jYT//7
/3rv29gZ2EuY2E/4+/98L+vYHNwLmN9P//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNh
P//v/euvb2BHYW5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhJf54YeLv/eufZaBnYSpjYT/07/3rvm9gZ2E
uY2E//+/9679vaGdhNmj9puey5au/VwMnYS5zYT//7H3rv2NgZ2EuY2E//+/9679vYHdhLnNqpuey5au/b0
pnIS5jdT//7/1rv29v52EuY2E//+/9679vYGdxLmNRNGNzIXN/b2BfYW5jYSf/7/3rP29gd2EuY2E//+/96
79vYGdhPmNhL/RzZLCkt6Bnei6jYT/j7/3rvm9gZ3GuY2E//+/9679vYGdhLnNhP+9v/eu/b2BnYS5jYT//
7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmN
hP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2
EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu
/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+
/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT/
/7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E6o0Gy0RpdYWRTD
YaKx2+h8lBesLmsO2O3R8AZ+BW8HC8my4lPiORv6/96508HV2jYpEDbILg9zb+bI/qsM6c7SK5zXwkoXJha
Output
time: 6ms
length: 41647
lines: 43
w...Ø¿ö±.ô.ì¶.
±í¾Õ..ÿÿ¿÷MZ.....ÿÿ..¸.....@.....È....º..´
Í!¸.LÍ!This program cannot be run in DOS mode.
$.....Aì¾3..Ò`..Ò`..Ò``ëÓa
.Ò`..Ó`c.Ò`.äÚa..Ò`.ã-
`..Ò`.äÐa..Ò`Rich..Ò`.....PE..L...Ûïg].....à.....,.....09.....@....
@.....@.....F.. ....
`..à.....p..l...PD..p.....@..
.....text....+.....,..... ..`.rdata..è
...@.....0.....@..@.data...¨....P.....>.....@..À.rsrc...à....
`.....@.....@..@.reloc..l....p.....B.....@..B.....
.....U.ì.ì.W.Á.UìS.Eè.øV..G.¶ð.þ võ<.sñ<-u
¹.....Mõë 3É.Mô<+u..¾7G.þ0u...<xt.


Recipe
From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars
To Hex
Delimiter
Space
Bytes per line
0
XOR
Key
bd819d84b98d84ffffbff7aefd
HEX
Scheme
Standard
Null preserving
To Hex
Delimiter
Space
Bytes per line
0
Input
length: 55532
lines: 1
ygIAAGEyck5SS3ZCSzAwcDhsAAAAAAAA46ctgZ6EuY2A//+/CFH9vTmdhLmNhP////eu/b2BnYS5jYT//7/
3rv29gZ2EuY2E//+/9679vYGdhLmNTP//v/mxR7OBKY10rDz+s3LW+pXU8r30y+LjjZ7S182c0+/y8Jnv4d
+NypmOlNOh2cvqremQm9rZo/C3pZ2EuY2E///+GxLOuAxP5LwAVp/6MiXOnVZS/I40X+T6cmyXzXBv4QlgY
+yEci3fY0rQ3YUQVtkZYC+eu3p8ne/o/uy8AFaf/7/3rv29gZ3U/I2Es/6693US2tydhLmNhP//vxeu/7yK
nIqpjaj//7/hrv29gZ2EibSE//+v9679/YGdhLnNhP/vv/eu/72Bm4S5jYT//7/xrv29gZ2EuY0E//+/867
9vYGdhLqNxHr/v+eu/a2BnYS5nYT/77/3rv29gY2EuY2E//+/9679vZnbhLkthP//v5eu/V2AnYS5jYT//7
/3rv29gZ2EuY2E/4+/98L+vYHNwLmN9P//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNh
P//v/euvb2BHYW5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhJf54YeLv/eufZaBnYSpjYT/07/3rvm9gZ2E
uY2E//+/9679vaGdhNmj9puey5au/VWMnYS5zYT//7H3rv2NgZ2EuY2E//+/9679vYHdhLnNqpuey5au/b0
pnIS5jdT//7/1rv29v52EuY2E//+/9679vYGdxLmNRNGNzIXN/b2BfYW5jYSf/7/3rP29gd2EuY2E//+/96
79vYGdhPmNhL/RzZLCkt6Bnei6jYT/j7/3rvm9gZ3GuY2E//+/9679vYGdhLnNhP+9v/eu/b2BnYS5jYT//
7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmN
hP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2
EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b
2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9
679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT/
/7/3rv29gZ2EuY2E//+/9679vYGdhLmNhP//v/eu/b2BnYS5jYT//7/3rv29gZ2EuY2E/6o0Gy0RpdYWRTD
YaKx2+h8lBesLmsO2O3R8AZ+BW8HC8my41PiORv6/96508HV2jYpEDbILg9zb+bI/qsM6c7SK5zXwkoXJha
Output
time: 44ms
length: 124940
lines: 1
77 83 9d 84 d8 bf f6 b1 ad f4 81 ec b6 8d b1 ed bc d5 8d 84 ff ff bf f7 4d 5a 90 00
03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
c8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72
61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65
2e 0d 0d 0a 24 00 00 00 00 00 00 00 41 ec bc 33 05 8d d2 60 05 8d d2 60 05 8d d2 60
60 eb d3 61 0a 8d d2 60 05 8d d3 60 63 8d d2 60 94 e4 da 61 00 8d d2 60 94 e4 2d 60

Do a little editing of the un-XOR-ed hex



Recipe

From Base64

Alphabet
A-Za-z0-9+/=

Remove non-alphabet chars

To Hex

Delimiter
Space

Bytes per line
0

From Hex

Delimiter
Auto

XOR

Key
aefdbd819d84b98d84ffffbff7

HEX

Scheme
Standard

Null preserving

Input

length: 124868
lines: 1

```
e3 a7 2d 81 9e 84 b9 8d 80 ff ff bf 08 51 fd bd 39 9d 84 b9 8d 84 ff ff ff f7 ae fd
bd 81 9d 84 b9 8d 84 ff ff bf f7 ae fd bd 81 9d 84 b9 8d 84 ff ff bf f7 ae fd bd 81
9d 84 b9 8d 4c ff ff bf f9 b1 47 b3 81 29 8d 74 ac 3c fe b3 72 d6 fa 95 d4 f2 bd f4
cb e2 e3 8d 9e d2 d7 cd 9c d3 ef f2 f0 99 ef e1 df 8d ca 99 8e 94 d3 a1 d9 cb ea ad
e9 90 9b da d9 a3 f0 b7 a5 9d 84 b9 8d 84 ff ff fe 1b 12 ce b8 0c 4f e4 bc 00 56 9f
fa 32 25 ce 9d 56 52 fc 8e 34 5f e4 fa 72 6c 97 cd 70 6f e1 09 60 63 ec 84 72 2d df
63 4a d0 dd 85 10 56 d9 19 60 2f 9e bb 7a 7c 9d ef e8 fe ec bc 00 56 9f ff bf f7 ae
fd bd 81 9d d4 fc 8d 84 b3 fe ba f7 75 12 da dc 9d 84 b9 8d 84 ff ff bf 17 ae ff bc
8a 9c 8a a9 8d a8 ff ff bf e1 ae fd bd 81 9d 84 89 b4 84 ff ff af f7 ae fd fd 81 9d
84 b9 cd 84 ff ef bf f7 ae ff bd 81 9b 84 b9 8d 84 ff ff bf f1 ae fd bd 81 9d 84 b9
8d 04 ff ff bf f3 ae fd bd 81 9d 84 ba 8d c4 7a ff bf e7 ae fd ad 81 9d 84 b9 9d 84
ff ef bf f7 ae fd bd 81 8d 84 b9 8d 84 ff ff bf f7 ae fd bd 99 db 84 b9 2d 84 ff ff
bf 97 ae fd 5d 80 9d 84 b9 8d 84 ff ff bf f7 ae fd bd 81 9d 84 b9 8d 84 ff 8f bf f7
c2 fe bd 81 cd c0 b9 8d f4 ff ff bf f7 ae fd bd 81 9d 84 b9 8d 84 ff ff bf f7 ae fd
bd 81 9d 84 b9 8d 84 ff ff bf f7 ae fd bd 81 9d 84 b9 8d 84 ff ff bf f7 ae bd bd 81
1d 85 b9 8d 84 ff ff bf f7 ae fd bd 81 9d 84 b9 8d 84 ff ff bf f7 ae fd bd 81 9d 84
97 f9 e1 87 8b bf f7 ae 7d 96 81 9d 84 a9 8d 84 ff d3 bf f7 ae f9 bd 81 9d 84 b9 8d
84 ff ff bf f7 ae fd bd a1 9d 84 d9 a3 f6 9b 9e cb 96 ae fd 55 8c 9d 84 b9 cd 84 ff
```

Output

time: 17ms
length: 41623
lines: 43

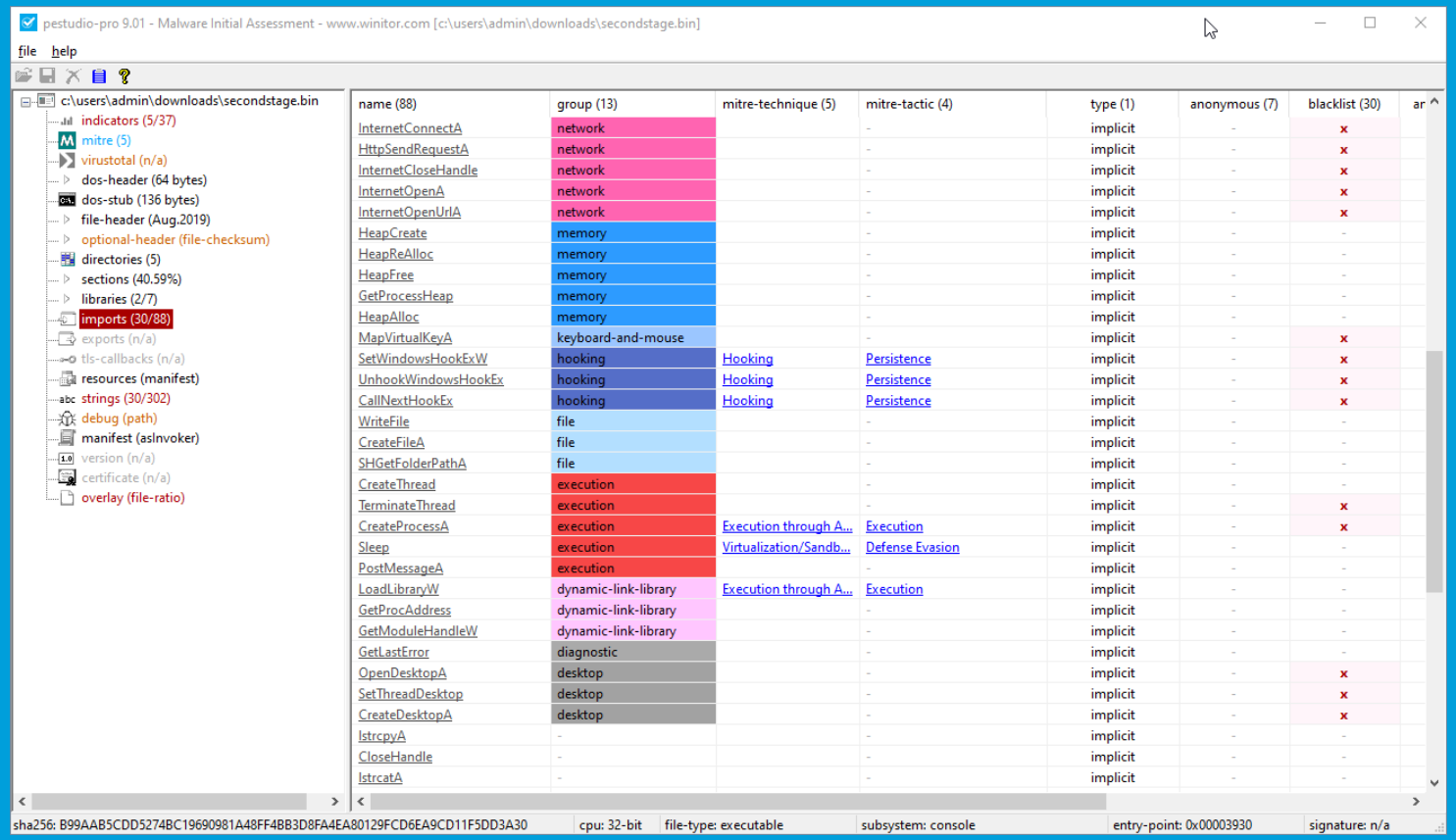
```
MZ.....ÿÿ..,.....@.....È.....º..´ Í!¸.LÍ!This
program cannot be run in DOS mode.

$.....Aì¼3..Ò`..Ò`..Ò``ëÓa
 Ò`..Ó`c Ò`.äÚa..Ò`.ã-
`..Ò`.äÐa..Ò`Rich..Ò`.....PE..L...Ûïg].....à.....,.....09.....@....
```

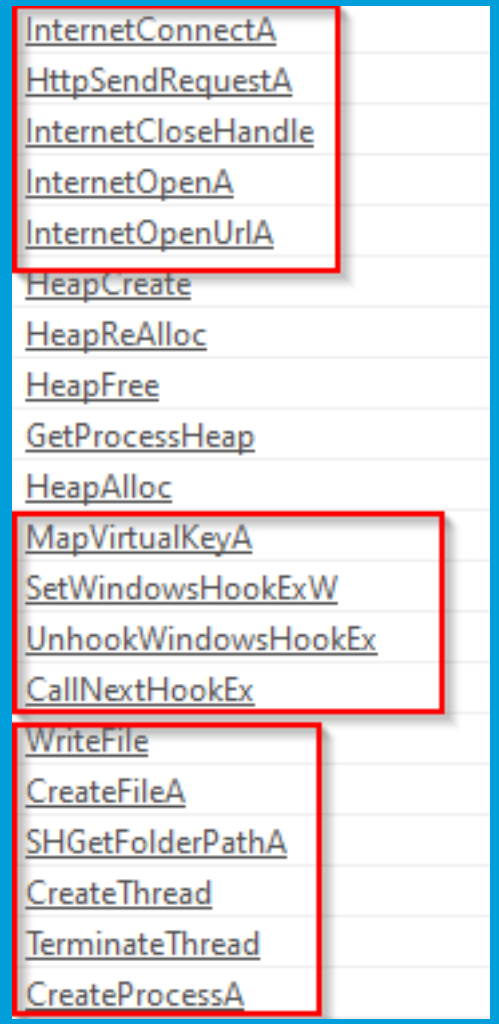

Interesting Strings/IOCs

```
POST
explorer.exe
Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0) Gecko/20100101 Firefox/47.0
51.81.9.201
Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
Admin
/test2/gateway.php
filename.exe
C:\Users\Dhillon\Desktop\Waifu's Work\Release\Waifu's Work.pdb
```

```
5|@@
h D@
F.QP
5X@@
0123456789abcdef
TaskbarGlomLevel
Shell_TrayWnd
\rundll32.exe shell32.dll,#61
Button
```

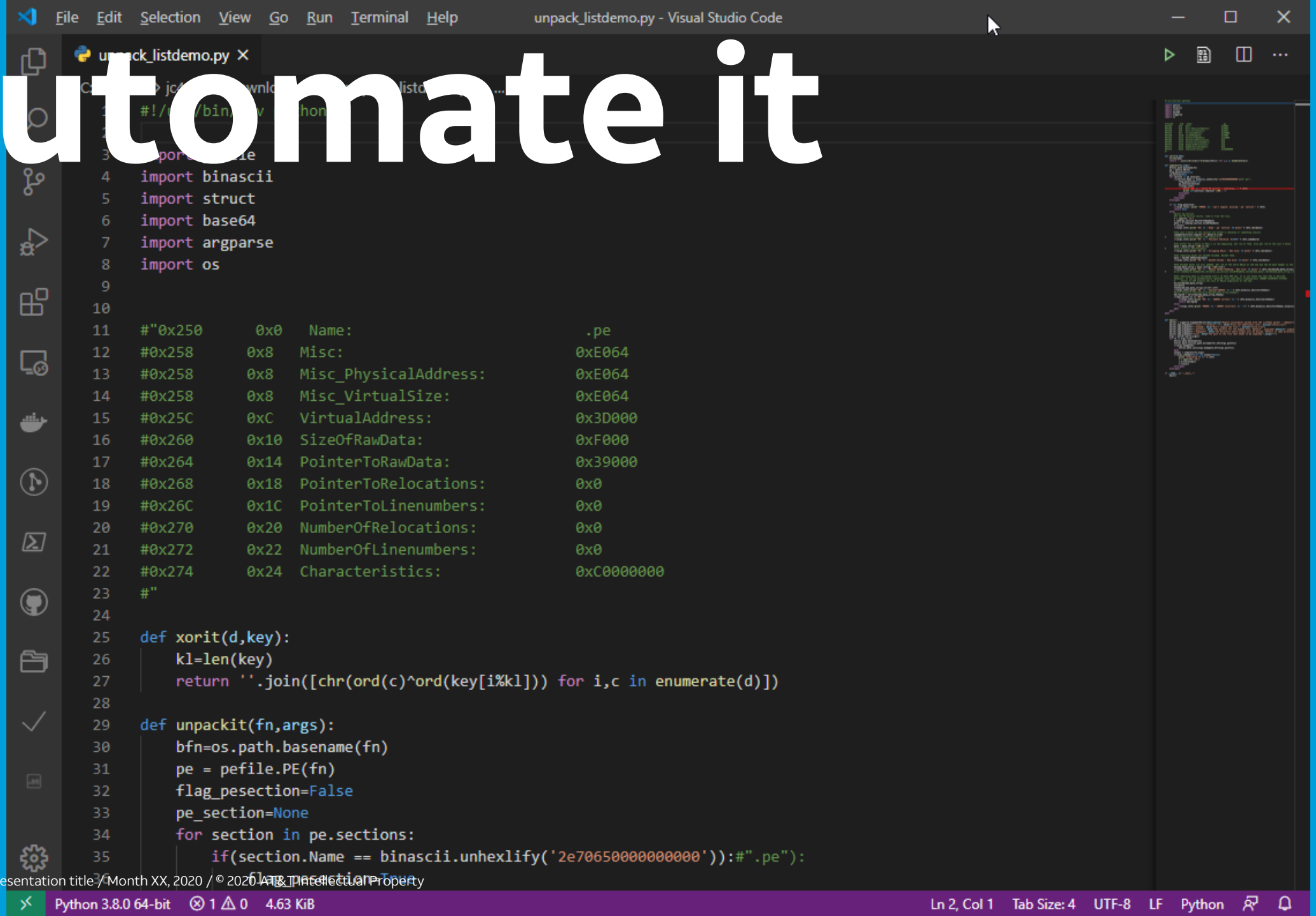

Looks like a key logger





AT&T

Automate it



AT&T

Conclusions

Questions?

References:

- https://github.com/att/docker-forensics/blob/master/unpack_listdemo.py

Contact me:

jac@att.com
jclausing@isc.sans.edu
@jclausing on twitter

Thanks for attending