Fireside Fridays

IP Addressing, Subnetting & data conversions
Week 7

Thanks to our sponsors!

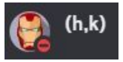
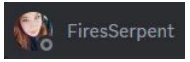
ACTIVE COUNTERMEASURES

BLACK HILLS Information Security • 2008 •

WILD WEST HACKIN' FEST

Antisyphon Training

Special Thanks to…

- Hermon 
(h,k)
    - Who will have a new job as a Cyber Threat Hunter in April :-)
- Emily 
FiresSerpent
- Both gave up many late nights to help with QA and development of this content
- Very much appreciate their efforts!
- Please give them a warm "thank you"

Lab requirements for this section

- Labs at the end
- All you need is a web browser

Classful routing

- Address space used to be classified as A, B and C
- Class used to ID network size being allocated
  - A = 17 million possible hosts
  - B = 65,000 possible hosts
  - C = 254 possible hosts
- Not very efficient - What if I need 1,000 addresses?
- Burned through available addresses very quickly
- Scrapped and replaced with CIDR
  - Classless Inter-Domain Routing
  - "/XX" designates the number of networking bits (explained later)

Reserved IP addresses

- 0.0.0.0 = This local network
- 10.0.0.0/8 = Private addressing
- 100.64.0.0/10 = Service provider private addressing
- 127.0.0.0/8 = Loopback, localhost
- 169.254.0.0/16 = link-local when no DHCP available
- 172.16.0.0/12 = Private addressing
- 192.168.0.0/16 = Private addressing
- 224.0.0.0/4 = Multicast communications
- 240.0.0.0/4 = Reserved for testing and future use
- 255.255.255.255/32 = Local network broadcast

How are addresses allocated?

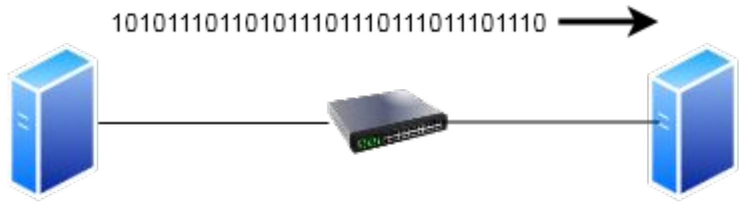
- Via the Internet Assigned Numbers Authority (IANA)
- Typically allocated to registry authorities
- Broken out by region
- These take care of allocations within their region

https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml

How are IP addresses formatted?

- Four groups of numbers
- Separated by periods
- Values are actually generated in binary
  - Only legal values are 1 or 0
  - Easy for computers to process
- We just view in decimal because it's easier for humans
- A "bit" is one value that can be either 1 or 0
- A "byte" is a collection of eight bits

It's all about the binary

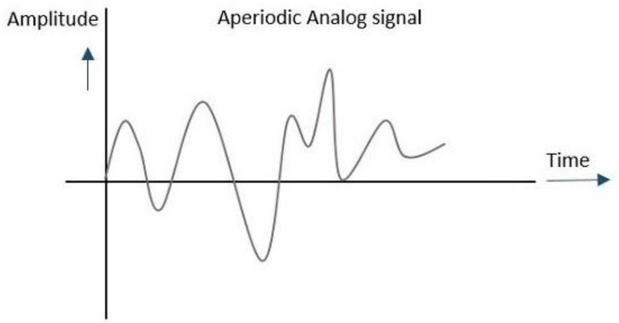


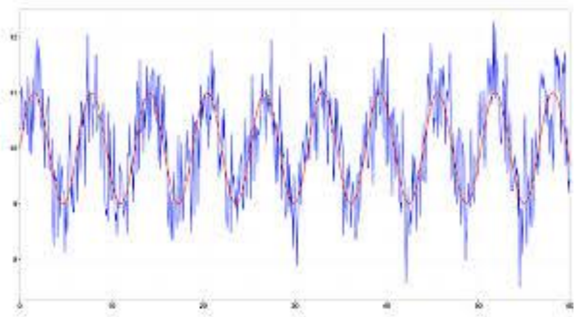
```
    10.55.182.100.14291 > 10.233.233.5.80: Flags [S], cksum 0x9309 (correct), 
seq
2643678933, win 64240, options [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0

        0x0000:  4500 0034 0a86 4000 7f06 3cb4 0a37 b664  E..4..@...<..7.d
        0x0010:  0ae9 e905 37d3 0050 9d93 56d5 0000 0000  ....7..P..V.....
        0x0020:  8002 faf0 9309 0000 0204 05b4 0103 0308  ................
        0x0030:  0101 0402                                ....
```

Why use binary?

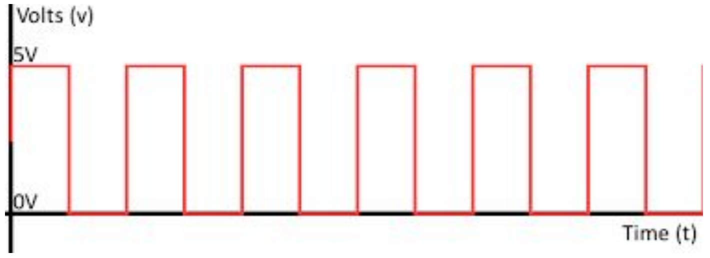
With noise

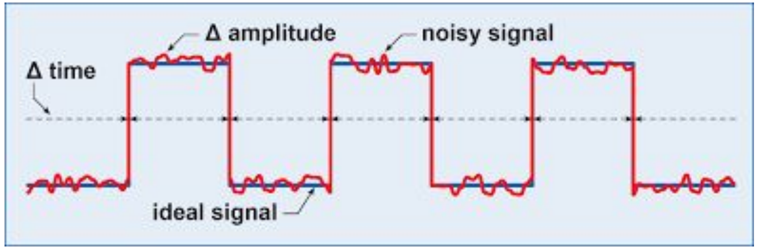
Analog



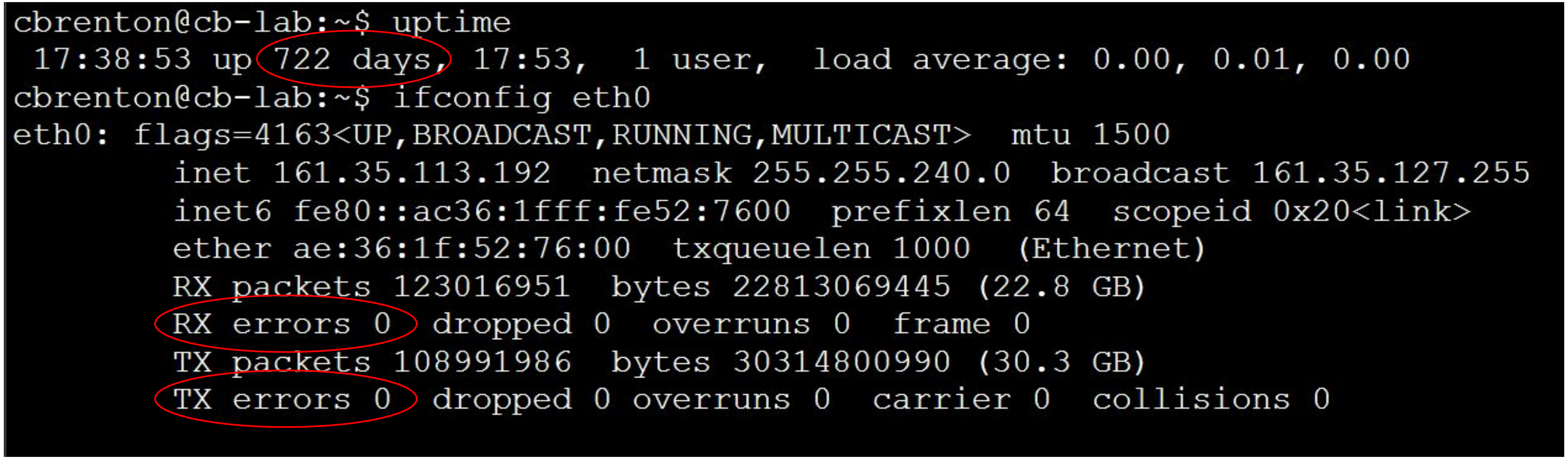


Digital





How often do we see digital errors?



```
cbrenton@cb-lab:~$ uptime
 17:38:53 up 722 days, 17:53,  1 user,  load average: 0.00, 0.01, 0.00
cbrenton@cb-lab:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 161.35.113.192  netmask 255.255.240.0  broadcast 161.35.127.255
        inet6 fe80::ac36:1fff:fe52:7600  prefixlen 64  scopeid 0x20<link>
        ether ae:36:1f:52:76:00  txqueuelen 1000  (Ethernet)
        RX packets 123016951  bytes 22813069445 (22.8 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 108991986  bytes 30314800990 (30.3 GB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

This is why we standardized on binary :-)

Binary to other formats

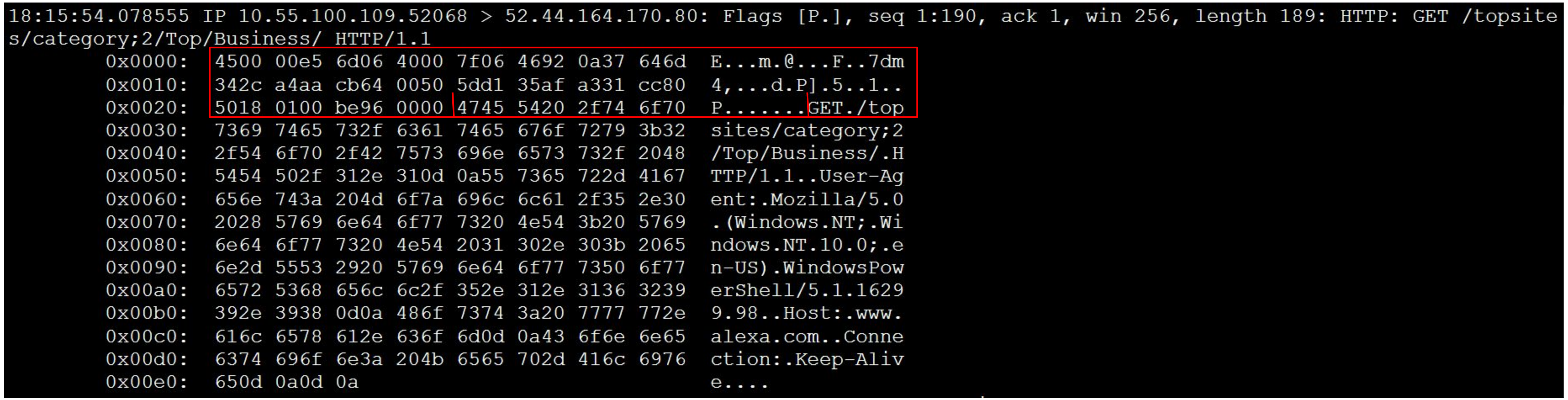
How to interpret the binary depends on the encoding being used.
Must be set in the software.

IP headers use decimal.
Payload uses ASCII.

Data sometimes displayed in Hex.
Tables used for conversion.

Binary	ASCII	Decimal	Hex
00000000	"null"	0	0x00
00000001	"start of header"	1	0x01
00110001	1	49	0x31
00110010	2	50	0x32
00110011	3	51	0x33
01000001	A	65	0x41
01000010	B	66	0x42
01000011	C	67	0x43
01100001	a	97	0x61
01100010	b	98	0x62
01100011	c	99	0x63
01111111	"DEL"	127	0x7F
11111111		255	0xFF

Wrong table, data looks scrambled



```
18:15:54.078555 IP 10.55.100.109.52068 > 52.44.164.170.80: Flags [P.], seq 1:190, ack 1, win 256, length 189: HTTP: GET /topsite
s/category;2/Top/Business/ HTTP/1.1
        0x0000:  4500 00e5 6d06 4000 7f06 4692 0a37 646d  E...m.@...F..7dm
        0x0010:  342c a4aa cb64 0050 5dd1 35af a331 cc80  4,...d.P].5..1..
        0x0020:  5018 0100 be96 0000 4745 5420 2f74 6f70  P.......GET./top
        0x0030:  7369 7465 732f 6361 7465 676f 7279 3b32  sites/category;2
        0x0040:  2f54 6f70 2f42 7573 696e 6573 732f 2048  /Top/Business/.H
        0x0050:  5454 502f 312e 310d 0a55 7365 722d 4167  TTP/1.1..User-Ag
        0x0060:  656e 743a 204d 6f7a 696c 6c61 2f35 2e30  ent:.Mozilla/5.0
        0x0070:  2028 5769 6e64 6f77 7320 4e54 3b20 5769  .(Windows.NT;.Wi
        0x0080:  6e64 6f77 7320 4e54 2031 302e 303b 2065  ndows.NT.10.0;.e
        0x0090:  6e2d 5553 2920 5769 6e64 6f77 7350 6f77  n-US).WindowsPow
        0x00a0:  6572 5368 656c 6c2f 352e 312e 3136 3239  erShell/5.1.1629
        0x00b0:  392e 3938 0d0a 486f 7374 3a20 7777 772e  9.98..Host:.www.
        0x00c0:  616c 6578 612e 636f 6d0d 0a43 6f6e 6e65  alexa.com..Conne
        0x00d0:  6374 696f 6e3a 204b 6565 702d 416c 6976  ction:.Keep-Aliv
        0x00e0:  650d 0a0d 0a                             e....
```

tcpdump decodes details as ASCII
But header info should be converted to decimal
Header info appears scrambled because wrong conversion

Converting 8 bits to decimal

Binary	1	0	1	0	1	0	1	0
Decimal	128	64	32	16	8	4	2	1

```
00000000 = 0
11111111 = 1+2+4+8+16+32+64+128 = 255
10101010 = 2+8+32+128 = 170
11110000 = 16+32+64+128 = 240
00101010 = 2+8+32 = 42
```

Speaking binary

- Bit - Single value that can only be 1 or 0
- Byte - A collection of 8 bits
- Nibble - A collection of 4 bits (half a byte)
- 32-bit word - Collection of 4 bytes
  - 4 bytes X 8 bits per byte = 32 bits
- Binary word can sometimes express other sizes
  - Usually linked to the CPU design

IPv4 addresses

- Combination of four bytes (8 bits in each, 32 bits total)
- Bytes are displayed separated by periods
- 255 greatest IP value because 11111111= decimal 255
- Subnet mask follows the same convention
- Corresponding subnet mask:
    - Binary "1" means network address
    - Binary "0" means host address

Subnet example

```
IP  192.168.0.10     11000000.10101000.00000000.00001010
Sub 255.255.255.0    11111111.11111111.11111111.00000000
```

Network   Host

Network bits are allocated from the left
Host bits are allocated from the right

Why do we care about binary?

- Matters when we get into subnetting
- Masking bits may not fall on an even byte boundary
- Last example had 24 masking bits (3x8)
  - What if there are 25 masking bits?
  - What if there are 23 masking bits?
  - Are 32 masking bits a valid value?
- Knowing binary can help with these calculations

CIDR format

- Identifies the number of masking bits
- Examples:
  - /8 = 255.0.0.0
  - /16 = 255.255.0.0
  - /23 = 255.255.254.0
  - /24 = 255.255.255.0
  - /25 = 255.255.255.128
  - /26 = 255.255.255.192

Why subnet?

- Lets you control network versus address allocation
- Increasing # of networks, decreases # of host per network
- Reducing # of networks, increases # of hosts per network
- For every network created, you lose two addresses:
  - 1 to label the network address (first address in the range)
  - 1 to label the network's broadcast address (last address in range)
  - This means you lose 2 host IPs per network

Let's go through an example

Assume I've been allocated 1.2.3.0/24

CIDR	Mask last byte	bits	# of nets	# hosts/net	Network addresses
/24	.0	00000000	1	254	.0
/25	.128	10000000	2	126	.0, .128
/26	.192	11000000	4	62	.0, .64, .128, .192
/30	.252	11111100	64	2	.4, .8, .12, .16, …. .240, .244, .248, .252
/31	.254	11111110	128	0	N/A
/32	.255	11111111	0	1	Special to match on exact IP address

Supernetting

Given: 1.2.2.0/23

Mask in binary = 11111111.11111111.11111110.00000000
Mask in decimal = 255.255.254.0
Network address = 1.2.2.0
Broadcast = 1.2.3.255
Number of usable host addresses = 510

Kind of a dead term since the change from class to CIDR

16 bit values

- As mentioned, 255 largest decimal value for a byte
- But wait, some fields can use larger numbers
- Example: valid port numbers are 0 - 65,535
- How do we express this in decimal?
- Answer: We combine two bytes, 16 bits in total

16 bit conversion

10101010-10101010

8192 1024 256 64 16 4 1

16384 2048 512 128 32 8 2

32768 4096

Max value = 65,535

Above binary converts to 43,690

Can we do weird masking?

- Is 11111111.10101010.01010101.00000000 a valid mask?
  - In decimal, this would be 255.170.85.0
- Technically yes, but assigning IPs would be a PITA
- Worked on older systems
- Doesn't seem to work on most modern systems
- Most use CIDR so not a possibility

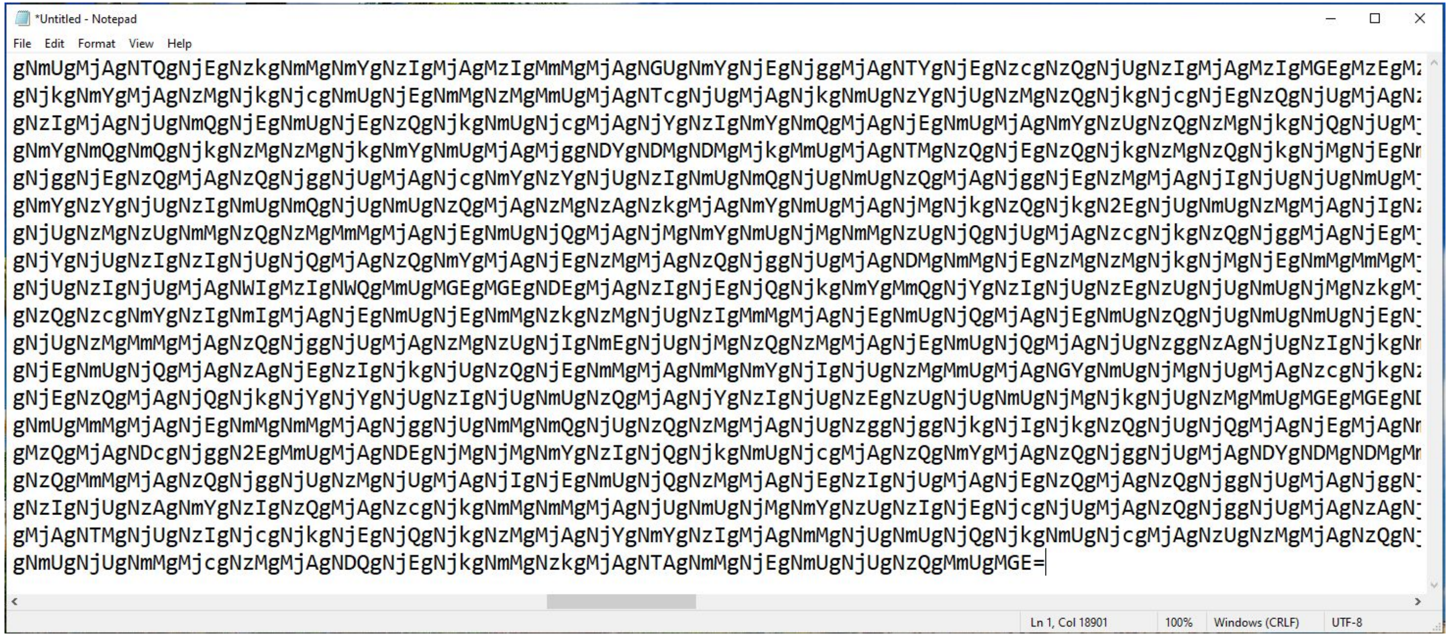
Obfuscation

- Attackers like to hide their data
- Most security tools based on pattern matching
  - I see "powershell" in the payload, that's bad
  - I see "70 6F 77 65 72 73 68 65 6C 6C" so that's OK
  - But wait, that's just powershell in Hex instead of ASCII
- Converting formats has less overhead than encryption
- Accomplishes the same goal of obfuscation
- Takes advantage of table expectication

Let's do a lab!

- Let's play a game of obfuscation
- Going to try and decode a hidden message
- Not encrypted, just taking advantage of table expectations
    - Your system will expect the data to decode as ASCII
    - Will actually be in a different format

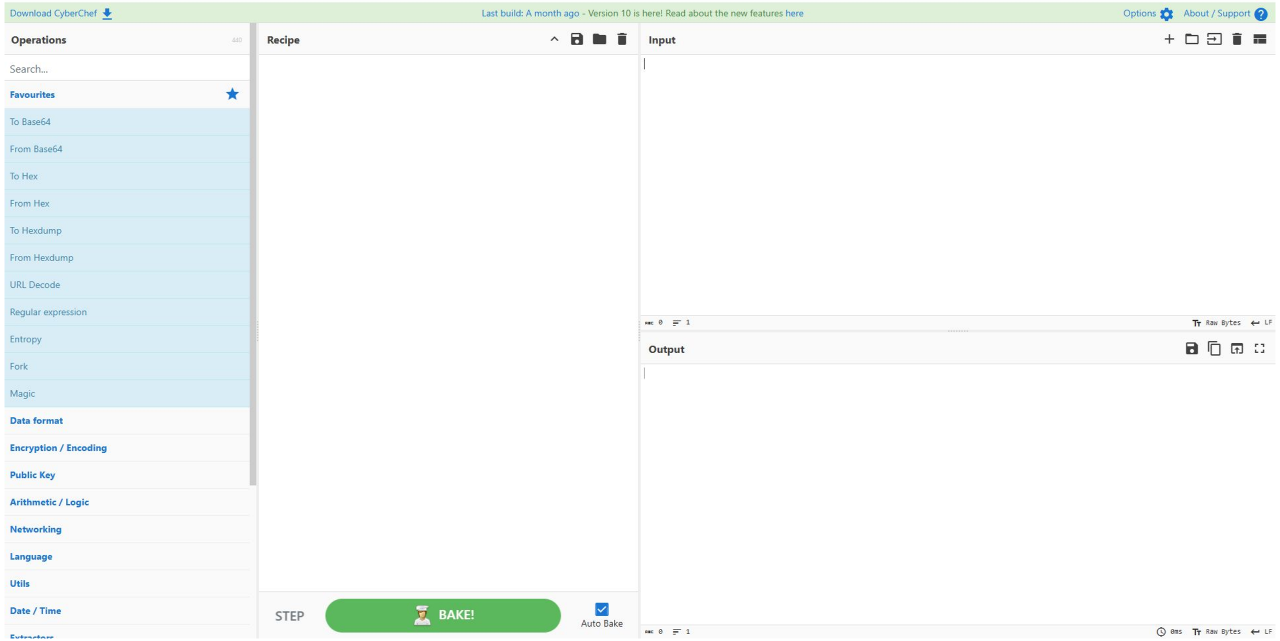
Download the super secret message



```
gNmUgMjAgNTQgNjEgNzkgNmMgNmYgNzIgMjAgMzIgMmMgMjAgNGUgNmYgNjEgNjggMjAgNTYgNjEgNzcgNzQgNjUgNzIgMjAgMzIgMGEgMzEgM
gNjkgNmYgMjAgNzMgNjkgNjcgNmUgNjEgNmMgNzMgMmUgMjAgNTcgNjUgMjAgNjkgNmUgNzYgNjUgNzMgNzQgNjkgNjcgNjEgNzQgNjUgMjAgN
gNzIgMjAgNjUgNmQgNjEgNmUgNjEgNzQgNjkgNmUgNjcgMjAgNjYgNzIgNmYgNmQgMjAgNjEgNmUgMjAgNmYgNzUgNzQgNzMgNjkgNjQgNjUgM
gNmYgNmQgNmQgNjkgNzMgNzMgNjkgNmYgNmUgMjAgMjggNDYgNDMgNDMgMjkgMmUgMjAgNTMgNzQgNjEgNzQgNjkgNzMgNzQgNjkgNjMgNjEgN
gNjggNjEgNzQgMjAgNzQgNjggNjUgMjAgNjcgNmYgNzYgNjUgNzIgNmUgNmQgNjUgNmUgNzQgMjAgNjggNjEgNzMgMjAgNjIgNjUgNjUgNmUgM
gNmYgNzYgNjUgNzIgNmUgNmQgNjUgNmUgNzQgMjAgNzMgNzAgNzkgMjAgNmYgNmUgMjAgNjMgNjkgNzQgNjkgN2EgNjUgNmUgNzMgMjAgNjIgN
gNjUgNzMgNzUgNmMgNzQgNzMgMmMgMjAgNjEgNmUgNjQgMjAgNjMgNmYgNmUgNjMgNmMgNzUgNjQgNjUgMjAgNzcgNjkgNzQgNjggMjAgNjEgM
gNjYgNjUgNzIgNzIgNjUgNjQgMjAgNzQgNmYgMjAgNjEgNzMgMjAgNzQgNjggNjUgMjAgNDMgNmMgNjEgNzMgNzMgNjkgNjMgNjEgNmMgMmMgM
gNjUgNzIgNjUgMjAgNWIgMzIgNWQgMmUgMGEgMGEgNDEgMjAgNzIgNjEgNjQgNjkgNmYgMmQgNjYgNzIgNjUgNzEgNzUgNjUgNmUgNjMgNzkgM
gNzQgNzcgNmYgNzIgNmIgMjAgNjEgNmUgNjEgNmMgNzkgNzMgNjUgNzIgMmMgMjAgNjEgNmUgNjQgMjAgNjEgNmUgNzQgNjUgNmUgNmUgNjEgN
gNjUgNzMgMmMgMjAgNzQgNjggNjUgMjAgNzMgNzUgNjIgNmEgNjUgNjMgNzQgNzMgMjAgNjEgNmUgNjQgMjAgNjUgNzggNzAgNjUgNzIgNjkgN
gNjEgNmUgNjQgMjAgNzAgNjEgNzIgNjkgNjUgNzQgNjEgNmMgMjAgNmMgNmYgNjIgNjUgNzMgMmUgMjAgNGYgNmUgNjMgNjUgMjAgNzcgNjkgN
gNjEgNzQgMjAgNjQgNjkgNjYgNjYgNjUgNzIgNjUgNmUgNzQgMjAgNjYgNzIgNjUgNzEgNzUgNjUgNmUgNjMgNjkgNjUgNzMgMmUgMGEgMGEgN
gNmUgMmMgMjAgNjEgNmMgNmMgMjAgNjggNjUgNmMgNmQgNjUgNzQgNzMgMjAgNjUgNzggNjggNjIgNjkgNzQgNjUgNjQgMjAgNjEgMjAgN
gMzQgMjAgNDcgNjggN2EgMmUgMjAgNDEgNjMgNjMgNmYgNzIgNjQgNjkgNmUgNjcgMjAgNzQgNmYgMjAgNzQgNjggNjUgMjAgNDYgNDMgNDMgM
gNzQgMmMgMjAgNzQgNjggNjUgNzMgNjUgMjAgNjIgNjEgNmUgNjQgNzMgMjAgNjEgNzIgNjUgMjAgNjEgNzQgMjAgNzQgNjggNjUgMjAgNjggN
gNzIgNjUgNzAgNmYgNzIgNzQgMjAgNzcgNjkgNmMgNmMgMjAgNjUgNmUgNjMgNmYgNzUgNzIgNjEgNjcgNjUgMjAgNzQgNjggNjUgMjAgNzAgN
gMjAgNTMgNjUgNzIgNjcgNjkgNjEgNjQgNjkgNzMgMjAgNjYgNmYgNzIgMjAgNmMgNjUgNmUgNjQgNjkgNmUgNjcgMjAgNzUgNzMgMjAgNzQgN
gNmUgNjUgNmMgMjcgNzMgMjAgNDQgNjEgNjkgNmMgNzkgMjAgNTAgNmMgNjEgNmUgNjUgNzQgMmUgMGE=
```

https://whats-this-stuff.s3.us-east-1.amazonaws.com/super-secret.txt

How do we decode this?



CyberChef to the rescue!
https://gchq.github.io/CyberChef/

What is CyberChef?

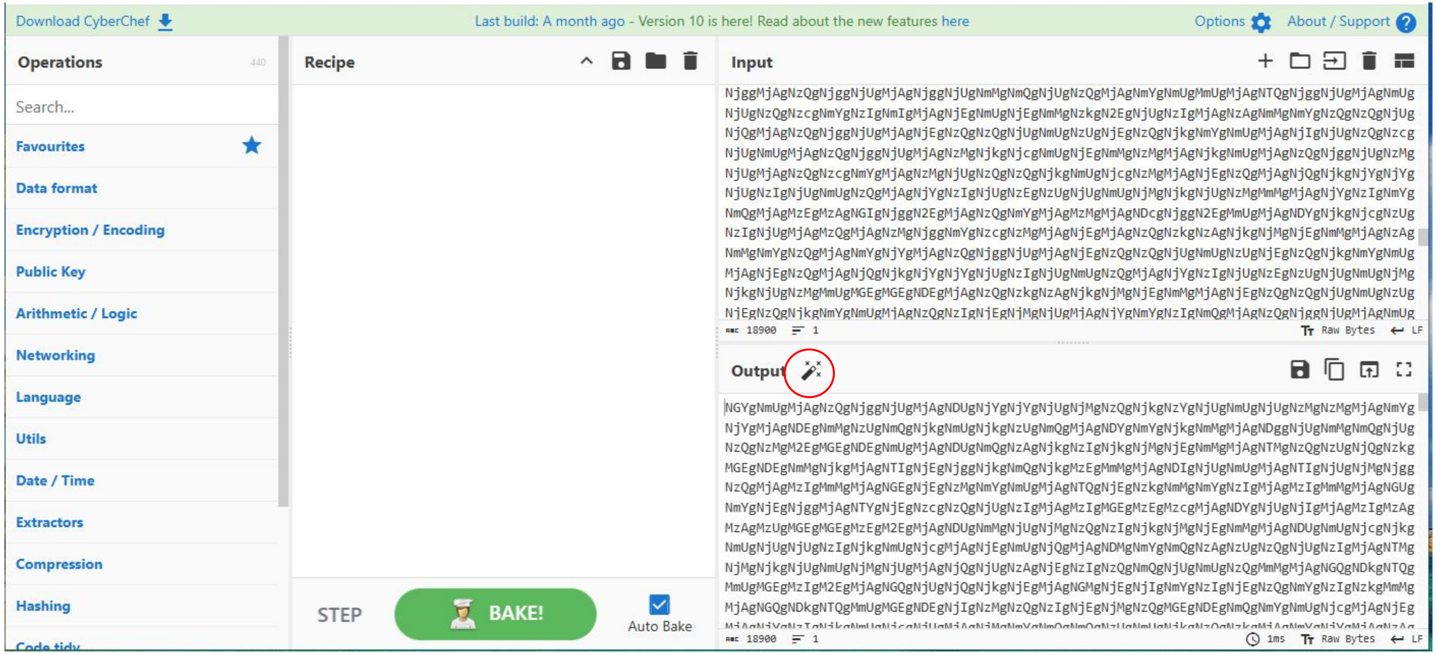
- Data conversion tool
- Can encode and decode in multiple formats
- Will even encrypt/decrypt data
- Can handle multiple layers of encoding
- Helpful encoding detection to simplify process
- Accessible online or run locally

```
sudo docker run -d --restart always -p 8000:8000
mpepping/cyberchef
```

Steps to perform

- Open browser tab for secret message
- Press "CTRL-a" then "CTRL-c" to select and copy
- Open browser tab for CyberChef
- Click mouse in "Input" frame
- Press "CTRL-v" to paste message

What you should see



```
NjggMjAgNzQgNjggNjUgMjAgNjggNjUgNmMgNmQgNjUgNzQgMjAgNmYgNmUgMmUgMjAgNTQgNjggNjUgMjAgNmUg
NjUgNzQgNzcgNmYgNzIgNmIgMjAgNjEgNmUgNjEgNmMgNzkgN2EgNjUgNzIgMjAgNzAgNmMgNmYgNzQgNzQgNjUg
NjQgMjAgNzQgNjggNjUgMjAgNjEgNzQgNzQgNjUgNmUgNzUgNjEgNzQgNjkgNmYgNmUgMjAgNjIgNjUgNzQgNzcg
NjUgNmUgMjAgNzQgNjggNjUgMjAgNzMgNjkgNjcgNmUgNjEgNmMgNzMgMjAgNjkgNmUgMjAgNzQgNjggNjUgNzMg
NjUgMjAgNzQgNzcgNmYgMjAgNzMgNjUgNzQgNzQgNjkgNmUgNjcgNzMgMjAgNjEgNzQgMjAgNjQgNjkgNjYgNjYg
NjUgNzIgNjUgNmUgNzQgMjAgNjYgNzIgNjUgNzEgNzUgNjUgNmUgNjMgNjkgNjUgNzMgMmMgMjAgNjYgNzIgNmYg
NmQgMjAgMzEgMzAgNGIgNjggN2EgMjAgNzQgNmYgMjAgMzMgMjAgNDcgNjggN2EgMmUgMjAgNDYgNjkgNjcgNzUg
NzIgNjUgMjAgMzQgMjAgNzMgNjggNmYgNzcgNzMgMjAgNjEgMjAgNzQgNzkgNzAgNjkgNjMgNjEgNmMgMjAgNzAg
NmMgNmYgNzQgMjAgNmYgNjYgMjAgNzQgNjggNjUgMjAgNjEgNzQgNzQgNjUgNmUgNzUgNjEgNzQgNjkgNmYgNmUg
MjAgNjEgNzQgMjAgNjQgNjkgNjYgNjYgNjUgNzIgNjUgNmUgNzQgMjAgNjYgNzIgNjUgNzEgNzUgNjUgNmUgNjMg
NjkgNjUgNzMgMmUgMGEgMGEgNDEgMjAgNzQgNzkgNzAgNjkgNjMgNjEgNmMgMjAgNjEgNzQgNzQgNjUgNmUgNzUg
NjEgNzQgNjkgNmYgNmUgMjAgNzQgNzIgNjEgNjMgNjUgMjAgNjYgNmYgNzIgNmQgMjAgNzQgNjggNjUgMjAgNmUg
```

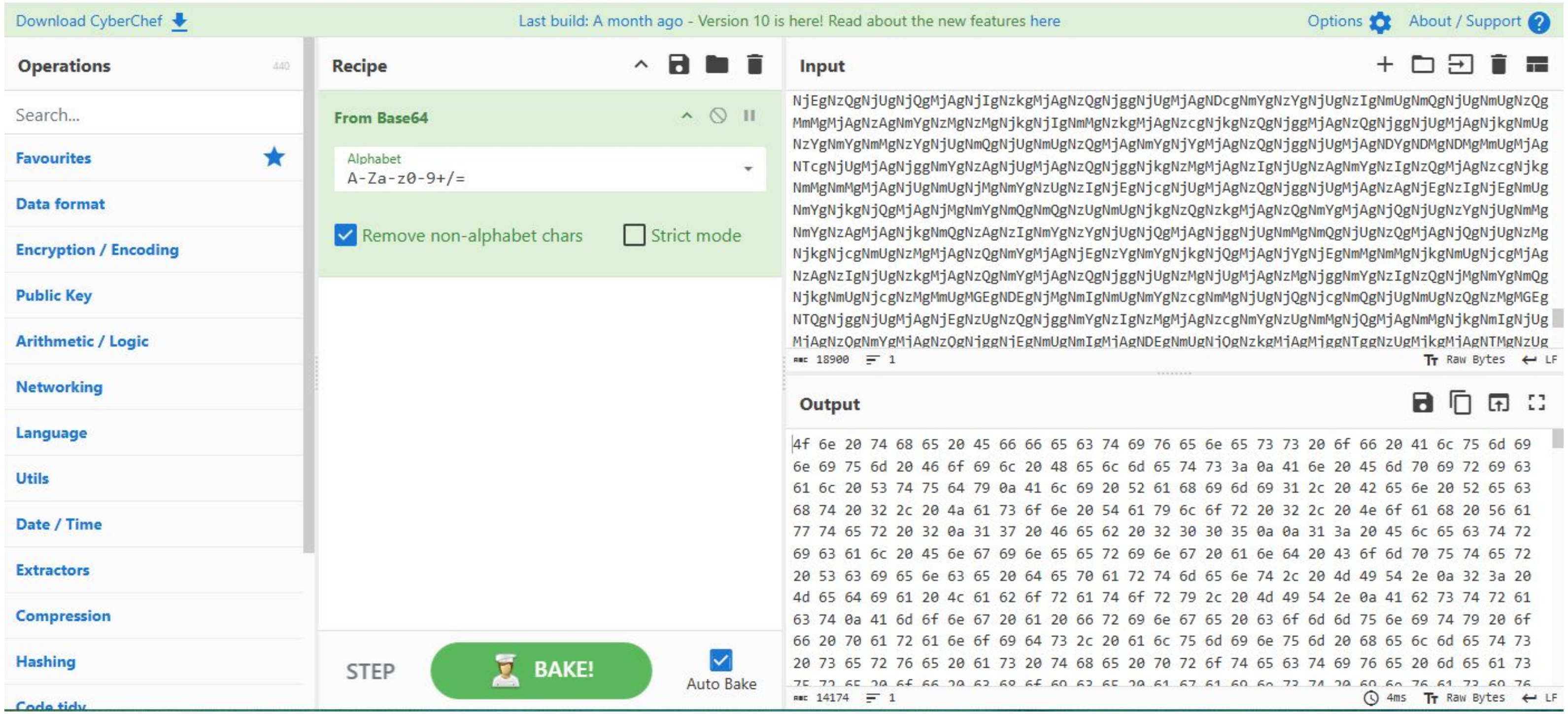
```
18900    1    Raw Bytes    LF
```

```
NGYgNmUgMjAgNzQgNjggNjUgMjAgNDUgNjYgNjYgNjUgNjMgNzQgNjkgNzYgNjUgNmUgNjUgNzMgNzMgMjAgNmYg
NjYgMjAgNDEgNmMgNzUgNmQgNjkgNmUgNjkgNzUgNmQgMjAgNDYgNmYgNjkgNmMgMjAgNDggNjUgNmMgNmQgNjUg
NzQgNzMgM2EgMGEgNDEgNmUgMjAgNDUgNmQgNzAgNjkgNzIgNjkgNjMgNjEgNmMgMjAgNTMgNzQgNzUgNjQgNzkg
MGEgNDEgNmMgNjkgMjAgNTIgNjEgNjggNjkgNmQgNjkgMzEgMmMgMjAgNDIgNjUgNmUgMjAgNTIgNjUgNjMgNjgg
NzQgMjAgMzIgMmMgMjAgNGEgNjEgNzMgNmYgNmUgMjAgNTQgNjEgNzkgNmMgNmYgNzIgMjAgMzIgMmMgMjAgNGUg
NmYgNjEgNjggMjAgNTYgNjEgNzcgNzQgNjUgNzIgMjAgMzIgMGEgMzEgMzcgMjAgNDYgNjUgNjIgMjAgMzIgMzAg
MzAgMzUgMGEgMGEgMzEgM2EgMjAgNDUgNmMgNjUgNjMgNzQgNzIgNjkgNjMgNjEgNmMgMjAgNDUgNmUgNjcgNjkg
NmUgNjUgNjUgNzIgNjkgNmUgNjcgMjAgNjEgNmUgNjQgMjAgNDMgNmYgNmQgNzAgNzUgNzQgNjUgNzIgMjAgNTMg
NjMgNjkgNjUgNmUgNjMgNjUgMjAgNjQgNjUgNzAgNjEgNzIgNzQgNmQgNjUgNmUgNzQgMmMgMjAgNGQgNDkgNTQg
MmUgMGEgMzIgM2EgMjAgNGQgNjUgNjQgNjkgNjEgMjAgNGMgNjEgNjIgNmYgNzIgNjEgNzQgNmYgNzIgNzkgMmMg
MjAgNGQgNDkgNTQgMmUgMGEgNDEgNjIgNzMgNzQgNzIgNjEgNjMgNzQgMGEgNDEgNmQgNmYgNmUgNjcgMjAgNjEg
```

```
18900    1    1ms    Raw Bytes    LF
```

Mouse over then click the magic wand

Hummm. That output looks like Hex



Alphabet
A-Za-z0-9+/=

[✓] Remove non-alphabet chars   [ ] Strict mode

Input

```
NjEgNzQgNjUgNjQgMjAgNjIgNzkgMjAgNzQgNjggNjUgMjAgNDcgNmYgNzYgNjUgNzIgNmUgNmQgNjUgNmUgNzQg
MmMgMjAgNzAgNmYgNzMgNzMgNjkgNjIgNmMgNzkgMjAgNzcgNjkgNzQgNjggMjAgNzQgNjggNjUgMjAgNjkgNmUg
NzYgNmYgNmMgNzYgNjUgNmQgNjUgNmUgNzQgMjAgNmYgNjYgMjAgNzQgNjggNjUgMjAgNDYgNDMgNDMgMmUgMjAg
NTcgNjUgMjAgNjggNmYgNzAgNjUgMjAgNzQgNjggNjkgNzMgMjAgNzIgNjUgNzAgNmYgNzIgNzQgMjAgNzcgNjkg
NmMgNmMgMjAgNjUgNmUgNjMgNmYgNzUgNzIgNjEgNjcgNjUgMjAgNzQgNjggNjUgMjAgNzAgNjEgNzIgNjEgNmUg
NmYgNjkgNjQgMjAgNjMgNmYgNmQgNmQgNzUgNmUgNjkgNzQgNzkgMjAgNzQgNmYgMjAgNjQgNjUgNzYgNjUgNmMg
NmYgNzAgMjAgNjkgNmQgNzAgNzIgNmYgNzYgNjUgNjQgMjAgNjggNjUgNmMgNmQgNjUgNzQgMjAgNjQgNjUgNzMg
NjkgNjcgNmUgNzMgMjAgNzQgNmYgMjAgNjEgNzYgNmYgNjkgNjQgMjAgNjYgNjEgNmMgNmMgNjkgNmUgNjcgMjAg
NzAgNzIgNjUgNzkgMjAgNzQgNmYgMjAgNzQgNjggNjUgNzMgNjUgMjAgNzMgNjggNmYgNzIgNzQgNjMgNmYgNmQg
NjkgNmUgNjcgNzMgMmUgMGEgNDEgNjMgNmIgNmUgNmYgNzcgNmMgNjUgNjQgNjcgNmQgNjUgNmUgNzQgNzMgMGEg
NTQgNjggNjUgMjAgNjEgNzUgNzQgNjggNmYgNzIgNzMgMjAgNzcgNmYgNzUgNmMgNjQgMjAgNmMgNjkgNmIgNjUg
MjAgNzQgNmYgMjAgNzQgNjggNjEgNmUgNmIgMjAgNDEgNmUgNjQgNzkgMjAgMjggNTggNzUgMjkgMjAgNTMgNzUg
```

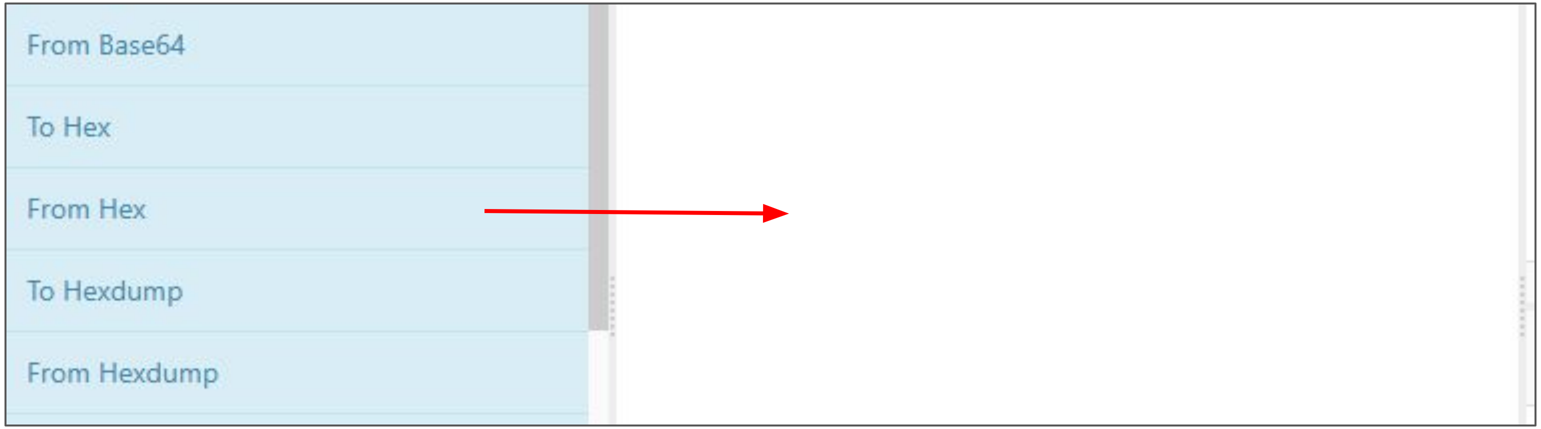
18900   1   Raw Bytes   LF

Output

```
4f 6e 20 74 68 65 20 45 66 66 65 63 74 69 76 65 6e 65 73 73 20 6f 66 20 41 6c 75 6d 69
6e 69 75 6d 20 46 6f 69 6c 20 48 65 6c 6d 65 74 73 3a 0a 41 6e 20 45 6d 70 69 72 69 63
61 6c 20 53 74 75 64 79 0a 41 6c 69 20 52 61 68 69 6d 69 31 2c 20 42 65 6e 20 52 65 63
68 74 20 32 2c 20 4a 61 73 6f 6e 20 54 61 79 6c 6f 72 20 32 2c 20 4e 6f 61 68 20 56 61
77 74 65 72 20 32 0a 31 37 20 46 65 62 20 32 30 30 35 0a 0a 31 3a 20 45 6c 65 63 74 72
69 63 61 6c 20 45 6e 67 69 6e 65 65 72 69 6e 67 20 61 6e 64 20 43 6f 6d 70 75 74 65 72
20 53 63 69 65 6e 63 65 20 64 65 70 61 72 74 6d 65 6e 74 2c 20 4d 49 54 2e 0a 32 3a 20
4d 65 64 69 61 20 4c 61 62 6f 72 61 74 6f 72 79 2c 20 4d 49 54 2e 0a 41 62 73 74 72 61
63 74 0a 41 6d 6f 6e 67 20 61 20 66 72 69 6e 67 65 20 63 6f 6d 6d 75 6e 69 74 79 20 6f
66 20 70 61 72 61 6e 6f 69 64 73 2c 20 61 6c 75 6d 69 6e 75 6d 20 68 65 6c 6d 65 74 73
20 73 65 72 76 65 20 61 73 20 74 68 65 20 70 72 6f 74 65 63 74 69 76 65 20 6d 65 61 73
75 72 65 20 6f 66 20 63 68 6f 69 63 65 20 61 67 61 69 6e 73 74 20 69 6e 76 61 73 69 76
```

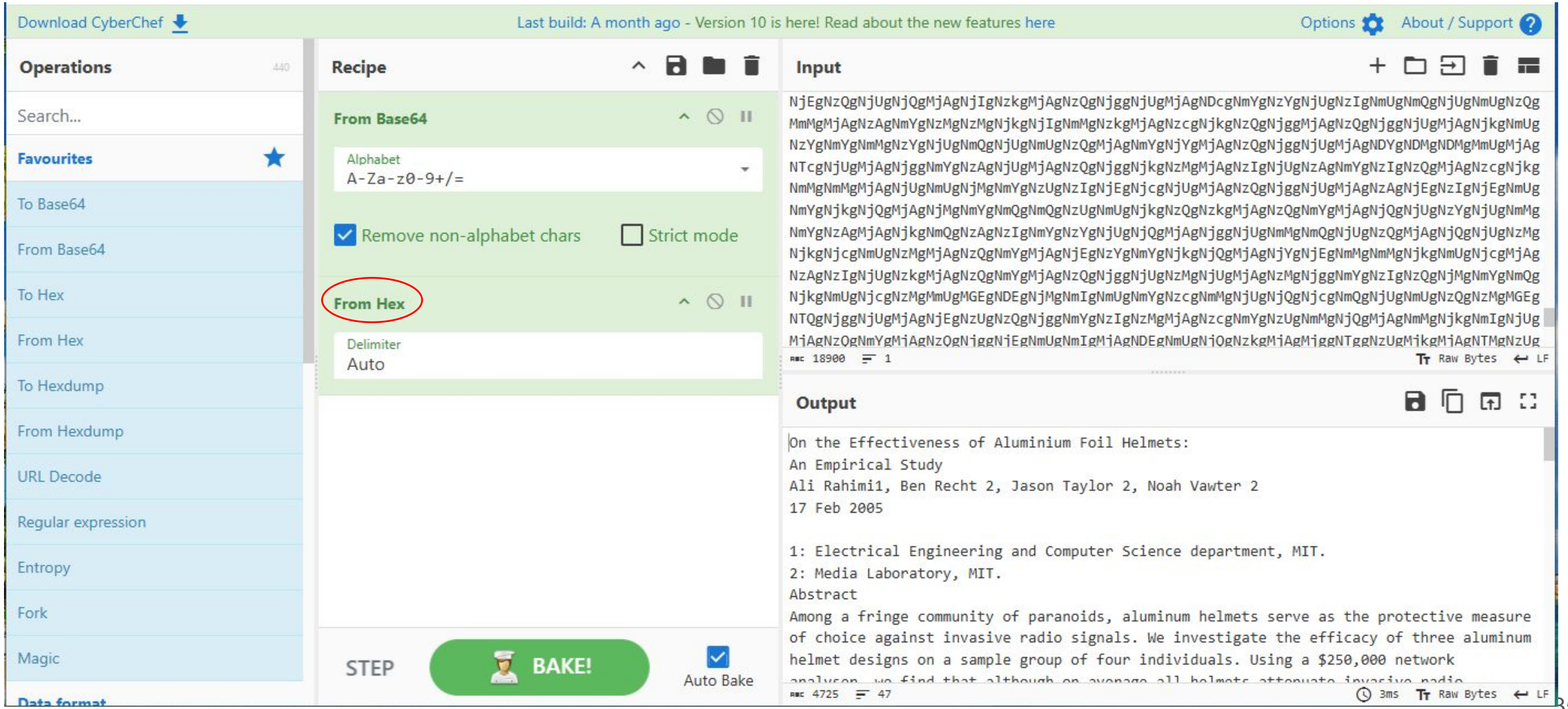
14174   1   4ms   Raw Bytes   LF

Decoding from Hex



Click "From Hex" and drag to the right

Score!



From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars [✓]
Strict mode [ ]

From Hex
Delimiter
Auto

```
NjEgNzQgNjUgNjQgMjAgNjIgNzkgMjAgNzQgNjggNjUgMjAgNDcgNmYgNzYgNjUgNzIgNmUgNmQgNjUgNmUgNzQg
MmMgMjAgNzAgNmYgNzMgNzMgNjkgNjIgNmMgNzkgMjAgNzcgNjkgNzQgNjggMjAgNzQgNjggNjUgMjAgNjkgNmUg
NzYgNmYgNmMgNzYgNjUgNmQgNjUgNmUgNzQgMjAgNmYgNjYgMjAgNzQgNjggNjUgMjAgNDYgNDMgNDMgMmUgMjAg
NTcgNjUgMjAgNjggNmYgNzAgNjUgMjAgNzQgNjggNjkgNzMgMjAgNzIgNjUgNzAgNmYgNzIgNzQgMjAgNzcgNjkg
NmMgNmMgMjAgNjUgNmUgNjMgNmYgNzUgNzIgNjEgNjcgNjUgMjAgNzQgNjggNjUgMjAgNzAgNjEgNzIgNjEgNmUg
NmYgNjkgNjQgMjAgNjMgNmYgNmQgNmQgNzUgNmUgNjkgNzQgNzkgMjAgNzQgNmYgMjAgNjQgNjUgNzYgNjUgNmMg
NmYgNzAgMjAgNjkgNmQgNzAgNzIgNmYgNzYgNjUgNjQgMjAgNjggNjUgNmMgNmQgNjUgNzQgMjAgNjQgNjUgNzMg
NjkgNjcgNmUgNzMgMjAgNzQgNmYgMjAgNjEgNzYgNmYgNjkgNjQgMjAgNjYgNjEgNmMgNmMgNjkgNmUgNjcgMjAg
NzAgNzIgNjUgNzkgMjAgNzQgNmYgMjAgNzQgNjggNjUgNzMgNjUgMjAgNzMgNjggNmYgNzIgNzQgNjMgNmYgNmQg
NjkgNmUgNjcgNzMgMmUgMGEgNDEgNjMgNmIgNmUgNmYgNzcgNmMgNjUgNjQgNjcgNmQgNjUgNmUgNzQgNzMgMGEg
NTQgNjggNjUgMjAgNjEgNzUgNzQgNjggNmYgNzIgNzMgMjAgNzcgNmYgNzUgNmMgNjQgMjAgNmMgNjkgNmIgNjUg
MjAgNzQgNmYgMjAgNzQgNjggNjEgNmUgNmIgMjAgNDEgNmUgNjQgNzkgMjAgNDIgNzIgNjEgNmUgNjQgMjAgNTMg
```

```
18900  1    Raw Bytes  LF
```

```
On the Effectiveness of Aluminium Foil Helmets:
An Empirical Study
Ali Rahimi1, Ben Recht 2, Jason Taylor 2, Noah Vawter 2
17 Feb 2005

1: Electrical Engineering and Computer Science department, MIT.
2: Media Laboratory, MIT.
Abstract
Among a fringe community of paranoids, aluminum helmets serve as the protective measure
of choice against invasive radio signals. We investigate the efficacy of three aluminum
helmet designs on a sample group of four individuals. Using a $250,000 network
```

```
4725  47    3ms  Raw Bytes  LF
```

Worth noting

- Most DLP's and IDS's would miss this
- Very few products will do the first level conversion
- Unaware of a product that would do 2nd level
- Allows attackers to go undetected
- With none of the encryption overhead

Tools to help

Conversion table:
https://www.ibm.com/docs/en/aix/7.2?topic=adapters-ascii-decimal-hexadecimal-octal-binary-conversion-table

IP calculator:
https://www.calculator.net/ip-subnet-calculator.html

Convert between multiple formats:
https://gchq.github.io/CyberChef/

Next week's Fireside Friday

- Packet sniffing tools!
- You will need:
    - Install Wireshark
    - Need tshark in your path
    - The decode1 pcap file
    - Optional - tcpdump

Wrap up

- Thank you for attending!
- Certs & video usually go out by Monday morning
- If you have any lingering questions, the Discord channel will remain active
  - Also a good chance to socialize with others in the class
  - Have other tips and tricks? Please share with others!