

HOW I "EARNED" (ANOTHER) SHMOOCON BARCODE

Tom Valadez
@tvldz

RECAP: SHMOOCON 2018 TICKET



Zack Fasel

@zfasel

Following



Looking for a @shmoocon ticket? I've hidden instructions for one somewhere on the internet on TCP/64531 #NotAJoke. First to find it wins it. Only 2 hints are 1) It's IPv4 and 2) It's somewhere in North America.

1:27 PM - 5 Jan 2018

2019 TICKET SALES DATA

So how fast did it sell out this year?

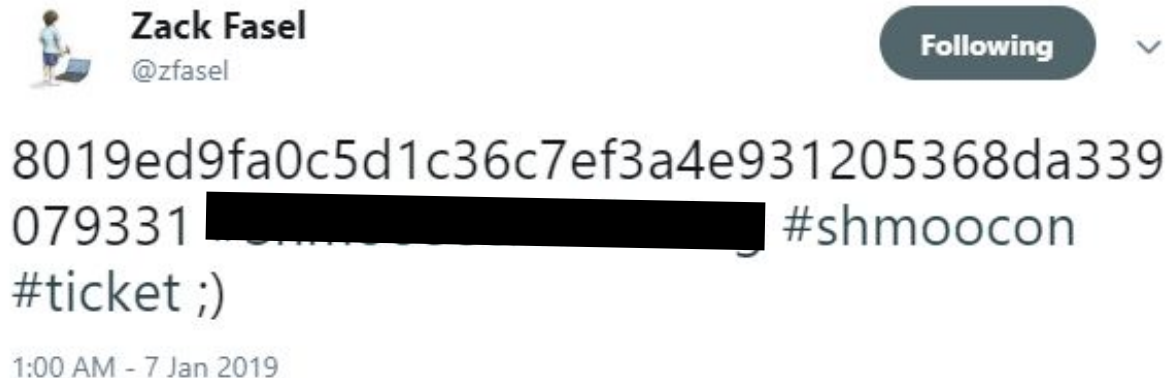
There were 1465 tickets released across all three rounds.

- All tickets were held in 17.13 seconds
- The waitlist filled up 2.53 seconds after that

In other words ShmooCon 2019 sold out in **19.66** seconds.

<https://shmoocon.org/2019/01/03/yearly-ticket-sales-stats-2019/>

MY "TICKET GUY"



NoVa Hackers FAQ:

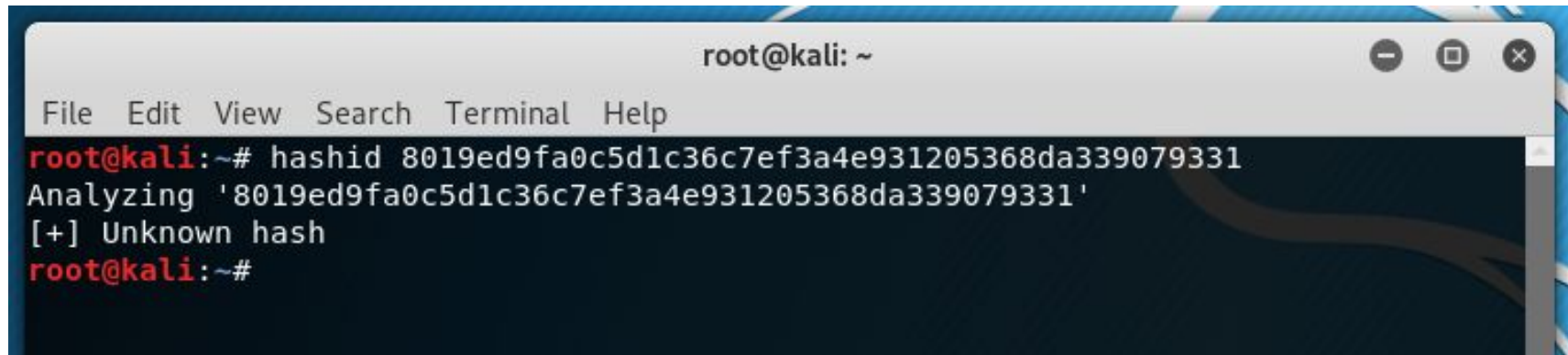
Q: Why have you hidden a hashtag in this slide?

A: Because I am slow and this journey requires that you be slow too.



8019ed9fa0c5d1c36c7ef3a4e931205368da339079331

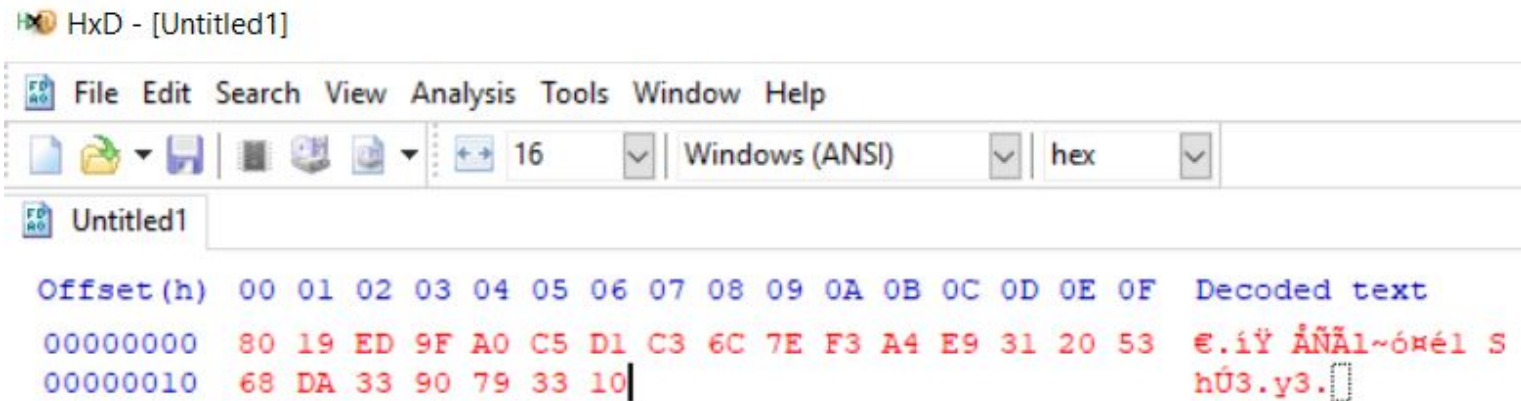
HASH?

A terminal window titled 'root@kali: ~' with standard window controls. The menu bar includes 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal shows the command 'hashid 8019ed9fa0c5d1c36c7ef3a4e931205368da339079331' being executed. The output indicates the hash is unknown.

```
root@kali:~# hashid 8019ed9fa0c5d1c36c7ef3a4e931205368da339079331
Analyzing '8019ed9fa0c5d1c36c7ef3a4e931205368da339079331'
[+] Unknown hash
root@kali:~#
```

WHAT INPUT WOULD WE BE SEARCHING FOR?

HxD: ENCODED DATA?



WOLFRAM ALPHA

0x8019ed9fa0c5d1c36c7ef3a4e931205368da339079331

Browse Examples

Surprise Me

Input interpretation:

8019ed9fa0c5d1...₁₆ (45 digits)

Open code

Decimal form:

766 854 076 538 060 022 587 270 218 734 525 792 632 165 847 301 329 713

Other base conversions:

Show exponent form

Show digit key

Fewer digits

More bases

1000000000011001111011011001111110100000110001011101000111000011011;
0110001111110111100111010010011101001001100010010000001;
0100110110100011011010001100111001000001111001001100110;
001₂

2000012132312133220030113101300312301332330322103221030102001103122;
03122030321001321030301₄

400147554772030564341554375716447223044024664332147101711461₈

a14139b8514457498a164271806a823617180a9bb80b5a9095₁₂

Other data types:

Big-endian

More

	hexadecimal value
unsigned 16-bit integer	3193 (overflow: truncated to 16 bits)
unsigned 32-bit integer	31930739 (overflow: truncated to 32 bits)
IEEE double-precision number	ba18f4b33d03204b

(assuming little-endian byte ordering)

Unit conversions for 8019ed9fa0c5d1...₁₆ (45 digits) bits:

9.586 × 10⁵² bytes

7.669 × 10⁵³ bits

180 bits

FILE? 0x80 0x19 0xED



Article

Talk

List of file signatures

From Wikipedia, the free encyclopedia

This is a [dynamic list](#) and may never be able

 2A 5F D7		0	cin	Kodak Cineon image
--------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------	---	-----	--------------------

ASSEMBLY?

x86:

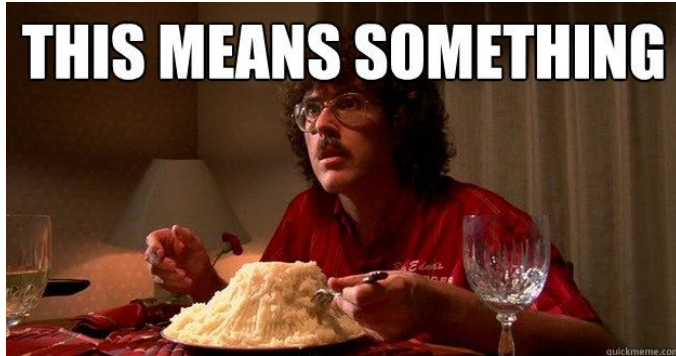
.data:00000000	8019ed	sbb BYTE PTR [ecx],0xed
.data:00000003	9f	lahf
.data:00000004	a0c5d1c36c	mov al,ds:0x6cc3d1c5
.data:00000009	7ef3	jle loc_fffffffe
.data:0000000b	a4	movs BYTE PTR es:[edi],BYTE PTR ds:[esi]
.data:0000000c	e931205368	jmp loc_68532042
.data:00000011	da33	fdiv DWORD PTR [ebx]
.data:00000013	90	nop
.data:00000014	7933	jns loc_00000049
.data:00000016	10	.byte 0x10

ACTUALLY STARING AT ACTUAL BITS FOR "CLUES"

Can I align the bits?

Is there an image there?

IS THAT A bitmap QR CODE?



Untitled - Notepad
File Edit Format View Help

```
10000000000011001111011  
0110011111101000001100  
0101110100011100001101  
1011000111111011110011  
1010010011101001001100  
0100100000010100110110  
1000110110100011001110  
0100000111100100110011  
000
```



OTHER THINGS I CONSIDERED:

- Searched for the string on Google, Social Media, etc.
- Considered other encoded data (IP Address?)
- Can I split the data? Is there a key AND ciphertext?
- **If this is all the information we have, can you think of anything else?**

This got me thinking about Information Theory and Sensory Deprivation

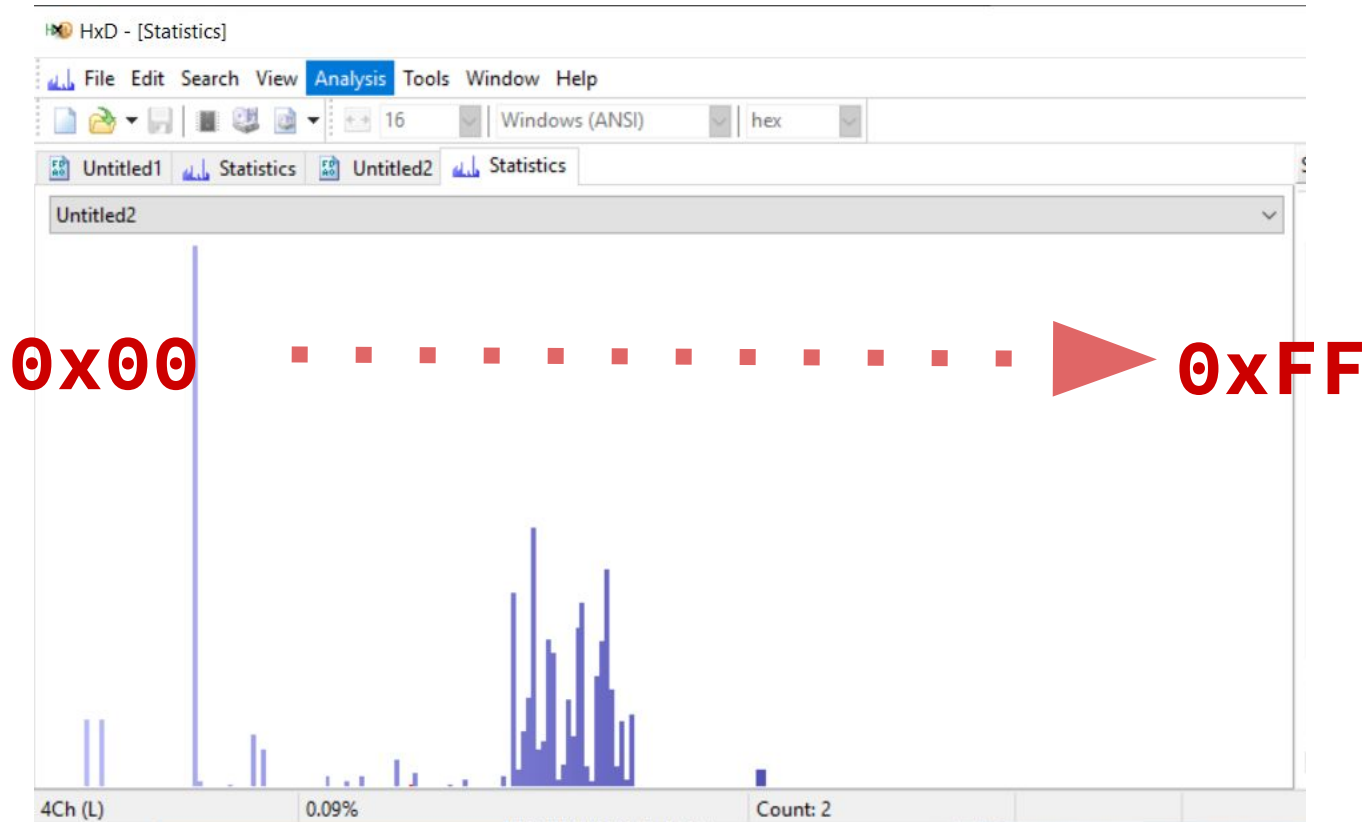


AM I MISSING INFORMATION?

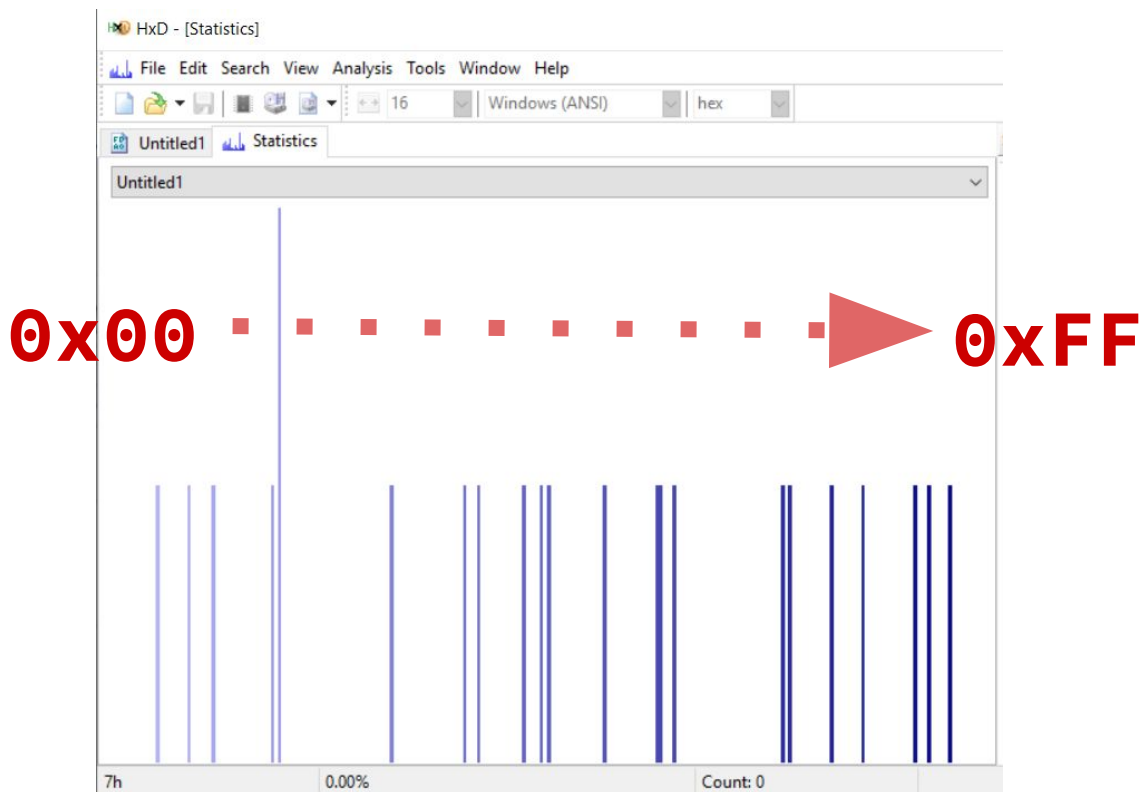
IS THIS INFORMATION RANDOM?

IS THIS CRYPTOGRAPHIC?

HxD "STATISTICS" TAB: PARAGRAPH FROM "PRIDE AND PREJUDICE" (ASCII):



HxD "STATISTICS" TAB FOR GIVEN VALUES: "EYEBALL ENTROPY"



BACK TO SQUARE ONE: #SHMOOSECRETSHARING



Zack Fasel

@zfasel

Following



8019ed9fa0c5d1c36c7ef3a4e931205368da339
079331 #ShmooSecretSharing #shmoocon
#ticket ;)

1:00 AM - 7 Jan 2019

SHAMIR'S SECRET SHARING

- Created by Adi Shamir (the S in RSA)
- Cryptographic Algorithm for “Secret Sharing”
- **Concept:**
 - Split a Secret into multiple parts “shares”
 - Define a “threshold,” which is the minimum number of shares required to reconstruct the original secret
 - Secret can be recreated with any combination of unique shares at the threshold

SHAMIR'S SECRET SHARING

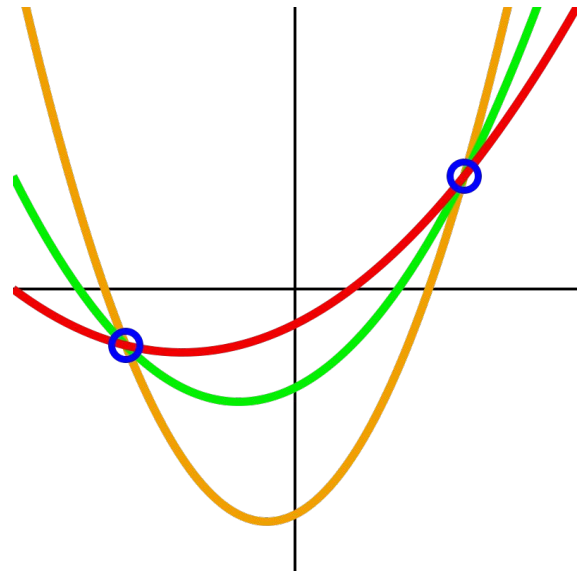
Example:

- **Secret:** Encoded in a 2nd Degree Polynomial (coefficient)
- **Each Share:** Points on the parabola

An infinite number of 2nd degree polynomials can pass through **two points**.

However, **three points** can define a unique 2nd degree polynomial

The actual implementation is more abstract (finite field), and can't be represented in 2 dimensions.



GOOGLE SEARCH FOR “#SHMOOSECRETSHARING”

Hits for:

- ShmooCon Slack
- Reddit
- LinkedIn
- GitHub
- Twitter
- Reddit
- YouTube

Shmoocon - Reddit

<https://www.reddit.com/r/Shmoocon/> ▼

and subscribe to one of thousands of communities. ×. 1. 1. 2. 3. **#ShmooSecretSharing** #shmoocon #ticket ;) (self.Shmoocon). submitted 2 months ago by zfasel.

#ShmooSecretSharing #shmoocon #ticket ;) - GitHub

<https://gist.github.com/zfasel/25ae4378e43cf24dfeeb3720208d64a5> ▼

Jan 7, 2019 - **#ShmooSecretSharing** #shmoocon #ticket ;). GitHub Gist: instantly share code, notes, and snippets.

#ShmooSecretSharing #shmoocon #ticket ;) - YouTube

<https://www.youtube.com/watch?v=t00Po7x2diE>



Jan 7, 2019 - Uploaded by Zack Fasel

805602e7c6ad7287b4c4b49754cf77b7f2021bf219fcb **#ShmooSecretSharing** #shmoocon #ticket ;)

Zack Fasel - YouTube

<https://www.youtube.com/channel/UCYXFilufQVv-9w3chWUc07g> ▼

#ShmooSecretSharing #shmoocon #ticket ;) - Duration: 28 seconds. 2 views; 21 minutes ago. 1:39:46.

Play next; Play now ...

IMPLEMENTATION MATTERS

- There are many different implementations of SSS
- The way the data is encoded varies.
- Secrets.js follows the same pattern as #ShmooconSecret Sharing (801XX, 802XX, etc)

Divide a 512-bit key, expressed in hexadecimal form, into 10 shares, requiring that any 5 of them are ne the original key:

```
// generate a 512-bit key
var key = secrets.random(512); // => key is a hex string

// split into 10 shares with a threshold of 5
var shares = secrets.share(key, 10, 5);
// => shares = ['801xxx...xxx', '802xxx...xxx', '803xxx...xxx', '804xxx...xxx', '805xxx...xxx']
```

[codahale/shamir: A Java implementation of Shamir's Secret ... - GitHub](https://github.com/codahale/shamir)

<https://github.com/codahale/shamir> ▼

A Java implementation of **Shamir's Secret Sharing** algorithm over GF(256). ... million developers working together to host and review **code**, manage projects, and ... **Shamir's Secret Sharing** algorithm is a way to split an arbitrary secret S into N ...

[ssss: Shamir's Secret Sharing Scheme - point-at-infinity.org](https://point-at-infinity.org/ssss/)

point-at-infinity.org/ssss/ ▼

Jan 2, 2018 - ssss is an implementation of **Shamir's secret sharing** scheme for UNIX/linux machines. It is free software, the **code** is licensed under the GNU ...

People also search for



[ssss github](#)

[ssss package](#)

[shamir secret sharing weaknesses](#)

[shamir secret sharing implementation python](#)

[shamir secret sharing blockchain](#)

[secret sharing schemes in cryptography pdf](#)

[Shamir's Secret Sharing — A numeric example walkthrough - Medium](https://medium.com/.../shamirs-secret-sharing-a-numeric-example-walkthrough-a59b2...)

<https://medium.com/.../shamirs-secret-sharing-a-numeric-example-walkthrough-a59b2...> ▼

Sep 22, 2018 - **Shamir's Secret Sharing** algorithm is an old cryptography algorithm (1979) invented by the Israeli cryptographer Adi Shamir (co-inventor of ...

[Shamir Secret Sharing Scheme - Ian Coleman](https://iancoleman.io/shamir/)

<https://iancoleman.io/shamir/> ▼

Shamir Secret Sharing Scheme. Split your secret into parts which can be combined back into the original secret using some or all of the parts.

[Shamir's Secret Sharing - kim hirokuni](https://kimh.github.io/blog/en/security/protect-your-secret-key-with-shamirs-secret-sharing/)

kimh.github.io/blog/en/security/protect-your-secret-key-with-shamirs-secret-sharing/ ▼

Shamir's secret sharing is an algorithm that divides a secret into shares. ... First get the **code** from PolyPassHash-Ruby and load shamirsecret.rb into your irb ...

[Shamir Secret Sharing - A Security Site](https://asecuritysite.com/encryption/shamir)

<https://asecuritysite.com/encryption/shamir> ▼

[Back] **Shamir's secret sharing** method generates a number of shares, of which a threshold defines the number of shares which can be used to re-build the ...

SECRETS.JS (PASSGUARDIAN.COM)

⚠ Not secure | passguardian.com

Reconstruct a secret

Instructions Reconstruct

Enter your shares:

808b4b5013a31a343a0a478857e67992c8b1ab8aeb3c6

805602e7c6ad7287b4c4b49754cf77b7f2021bf219fcb

806069f38c4b9ee93369a251701062a39f6f6b0f21e5a

8019ed9fa0c5d1c36c7ef3a4e931205368da339079331

Reset

Reconstructed secret

urba.ne/s3