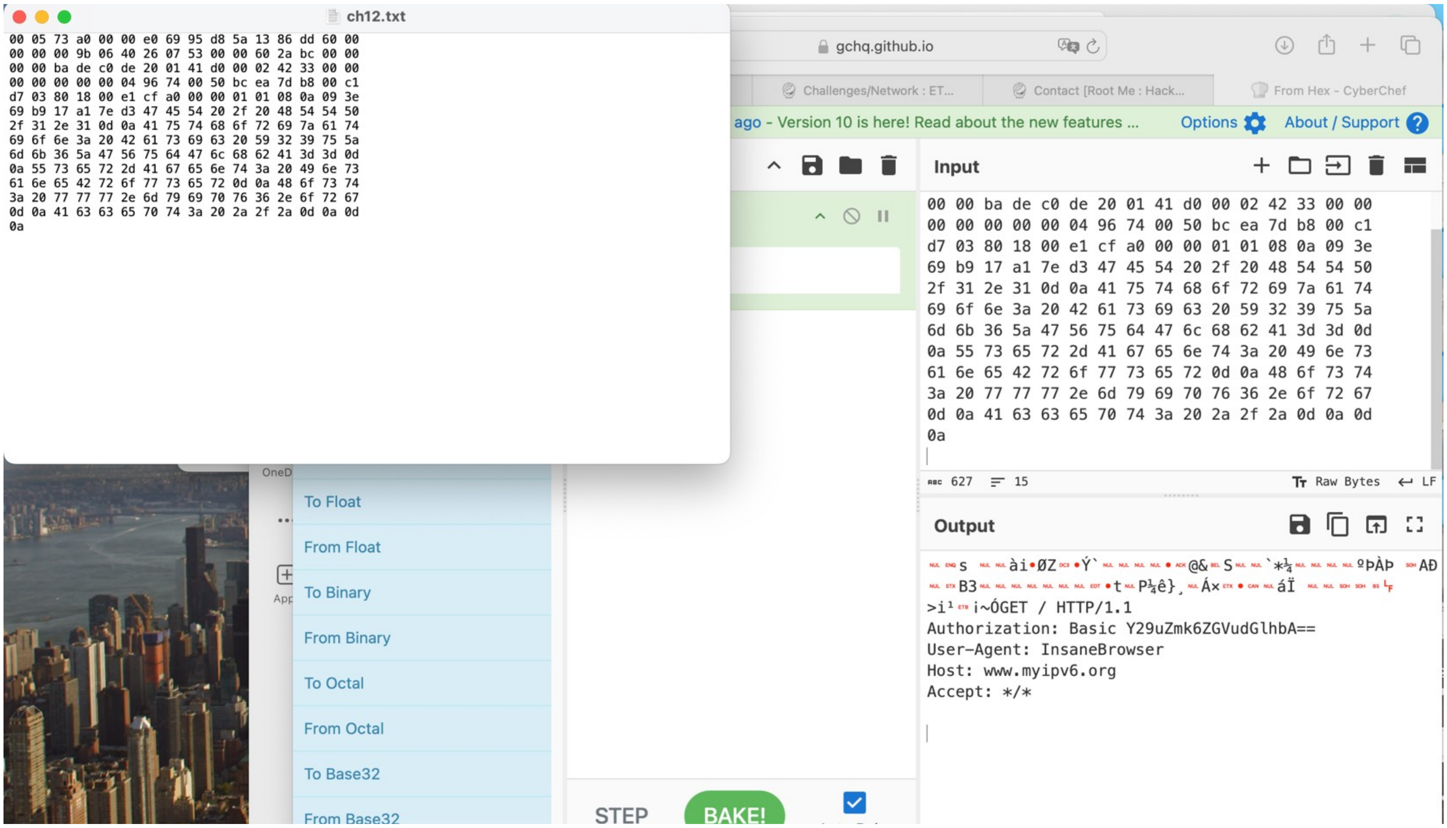
TSIS 5

Completed by Gaaze Verena, 22B030332

1. Root me: Ethernet -frame



ch12.txt

```
00 05 73 a0 00 00 e0 69 95 d8 5a 13 86 dd 60 00
00 00 00 9b 06 40 26 07 53 00 00 60 2a bc 00 00
00 00 ba de c0 de 20 01 41 d0 00 02 42 33 00 00
00 00 00 00 00 04 96 74 00 50 bc ea 7d b8 00 c1
d7 03 80 18 00 e1 cf a0 00 00 01 01 08 0a 09 3e
69 b9 17 a1 7e d3 47 45 54 20 2f 20 48 54 54 50
2f 31 2e 31 0d 0a 41 75 74 68 6f 72 69 7a 61 74
69 6f 6e 3a 20 42 61 73 69 63 20 59 32 39 75 5a
6d 6b 36 5a 47 56 75 64 47 6c 68 62 41 3d 3d 0d
0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 49 6e 73
61 6e 65 42 72 6f 77 73 65 72 0d 0a 48 6f 73 74
3a 20 77 77 77 2e 6d 79 69 70 76 36 2e 6f 72 67
0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 0d
0a
```

gchq.github.io — From Hex - CyberChef

Input

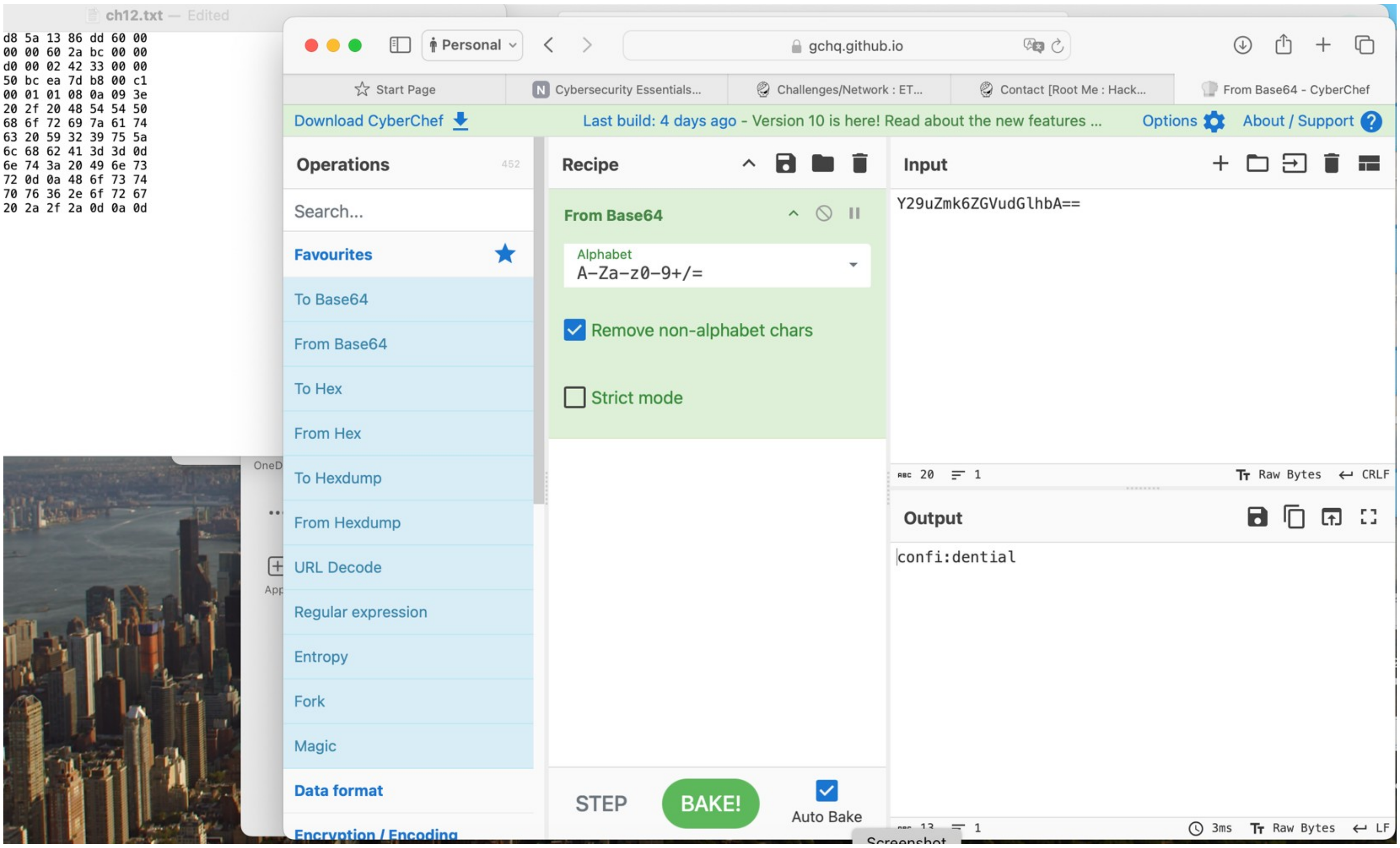
```
00 00 ba de c0 de 20 01 41 d0 00 02 42 33 00 00
00 00 00 00 00 04 96 74 00 50 bc ea 7d b8 00 c1
d7 03 80 18 00 e1 cf a0 00 00 01 01 08 0a 09 3e
69 b9 17 a1 7e d3 47 45 54 20 2f 20 48 54 54 50
2f 31 2e 31 0d 0a 41 75 74 68 6f 72 69 7a 61 74
69 6f 6e 3a 20 42 61 73 69 63 20 59 32 39 75 5a
6d 6b 36 5a 47 56 75 64 47 6c 68 62 41 3d 3d 0d
0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 49 6e 73
61 6e 65 42 72 6f 77 73 65 72 0d 0a 48 6f 73 74
3a 20 77 77 77 2e 6d 79 69 70 76 36 2e 6f 72 67
0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 0d
0a
```

abc 627 15 Raw Bytes LF

Output

```
NUL ENQ s NUL NUL ài•ØZ DC3 •Ý` NUL NUL NUL NUL • ACK @& BEL S NUL NUL `*¼ NUL NUL NUL NUL ºÞÀÞ SOH AÐ
NUL STX B3 NUL NUL NUL NUL NUL NUL NUL EOT •t NUL P¼ê}¸ NUL Á× ETX • CAN NUL áÏ NUL NUL SOH SOH BS LF
>i¹ ETB i~ÓGET / HTTP/1.1
Authorization: Basic Y29uZmk6ZGVudGlhbA==
User-Agent: InsaneBrowser
Host: www.myipv6.org
Accept: */*
```

To Float
From Float
To Binary
From Binary
To Octal
From Octal
To Base32
From Base32
STEP
BAKE!
ago - Version 10 is here! Read about the new features ...
Options
About / Support
Challenges/Network : ET...
Contact [Root Me : Hack...



ch12.txt — Edited

```
d8 5a 13 86 dd 60 00
00 00 60 2a bc 00 00
d0 00 02 42 33 00 00
50 bc ea 7d b8 00 c1
00 01 01 08 0a 09 3e
20 2f 20 48 54 54 50
68 6f 72 69 7a 61 74
63 20 59 32 39 75 5a
6c 68 62 41 3d 3d 0d
6e 74 3a 20 49 6e 73
72 0d 0a 48 6f 73 74
70 76 36 2e 6f 72 67
20 2a 2f 2a 0d 0a 0d
```

gchq.github.io — From Base64 - CyberChef

Recipe: From Base64

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

☑ Remove non-alphabet chars

□ Strict mode

Input

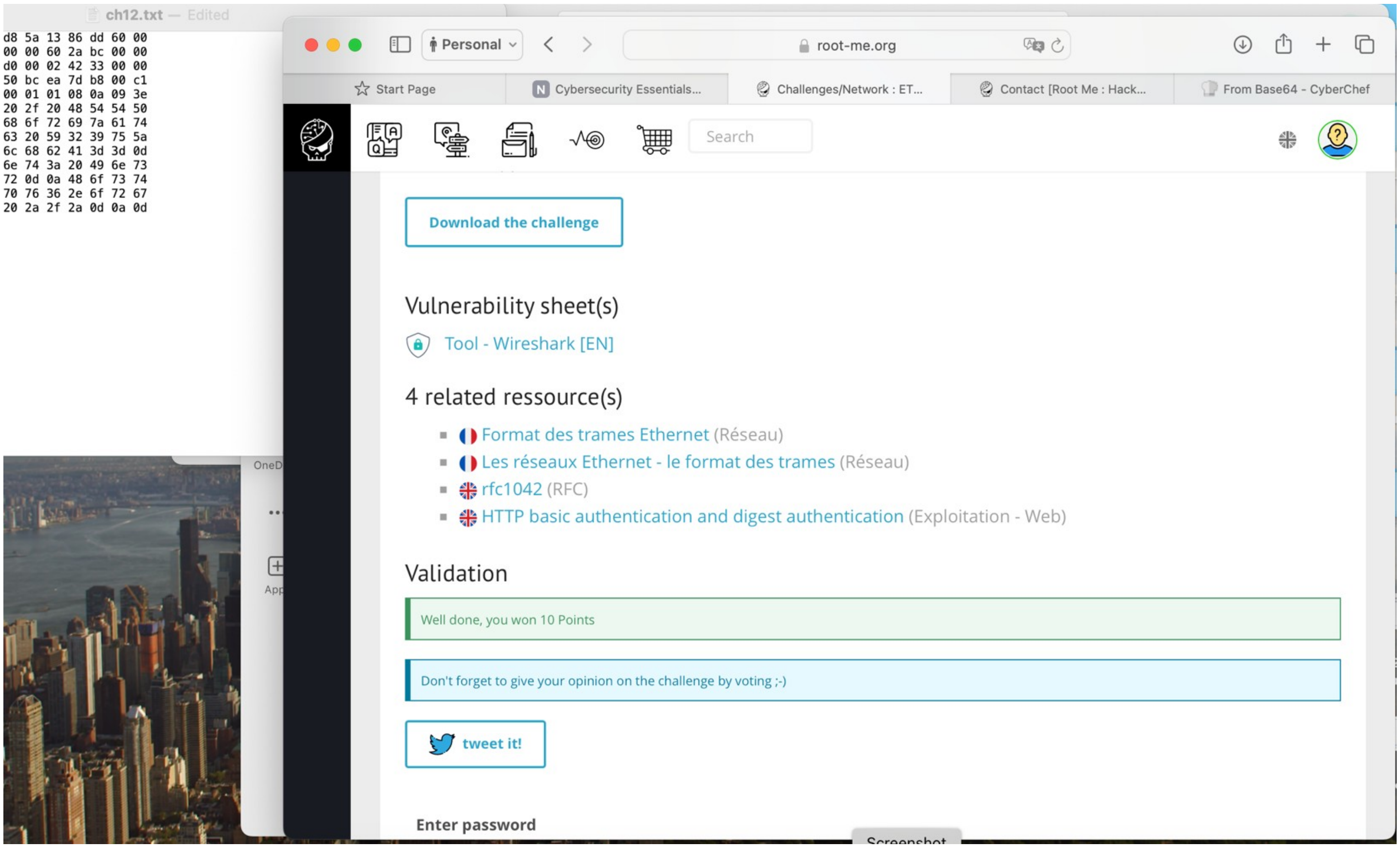
```
Y29uZmk6ZGVudGlhbA==
```

abc 20 1 Raw Bytes CRLF

Output

```
confi:dential
```

13 1 3ms Raw Bytes LF



```
d8 5a 13 86 dd 60 00
00 00 60 2a bc 00 00
d0 00 02 42 33 00 00
50 bc ea 7d b8 00 c1
00 01 01 08 0a 09 3e
20 2f 20 48 54 54 50
68 6f 72 69 7a 61 74
63 20 59 32 39 75 5a
6c 68 62 41 3d 3d 0d
6e 74 3a 20 49 6e 73
72 0d 0a 48 6f 73 74
70 76 36 2e 6f 72 67
20 2a 2f 2a 0d 0a 0d
```

Download the challenge

Vulnerability sheet(s)

Tool - Wireshark [EN]

4 related ressource(s)

- Format des trames Ethernet (Réseau)
- Les réseaux Ethernet - le format des trames (Réseau)
- rfc1042 (RFC)
- HTTP basic authentication and digest authentication (Exploitation - Web)

Validation

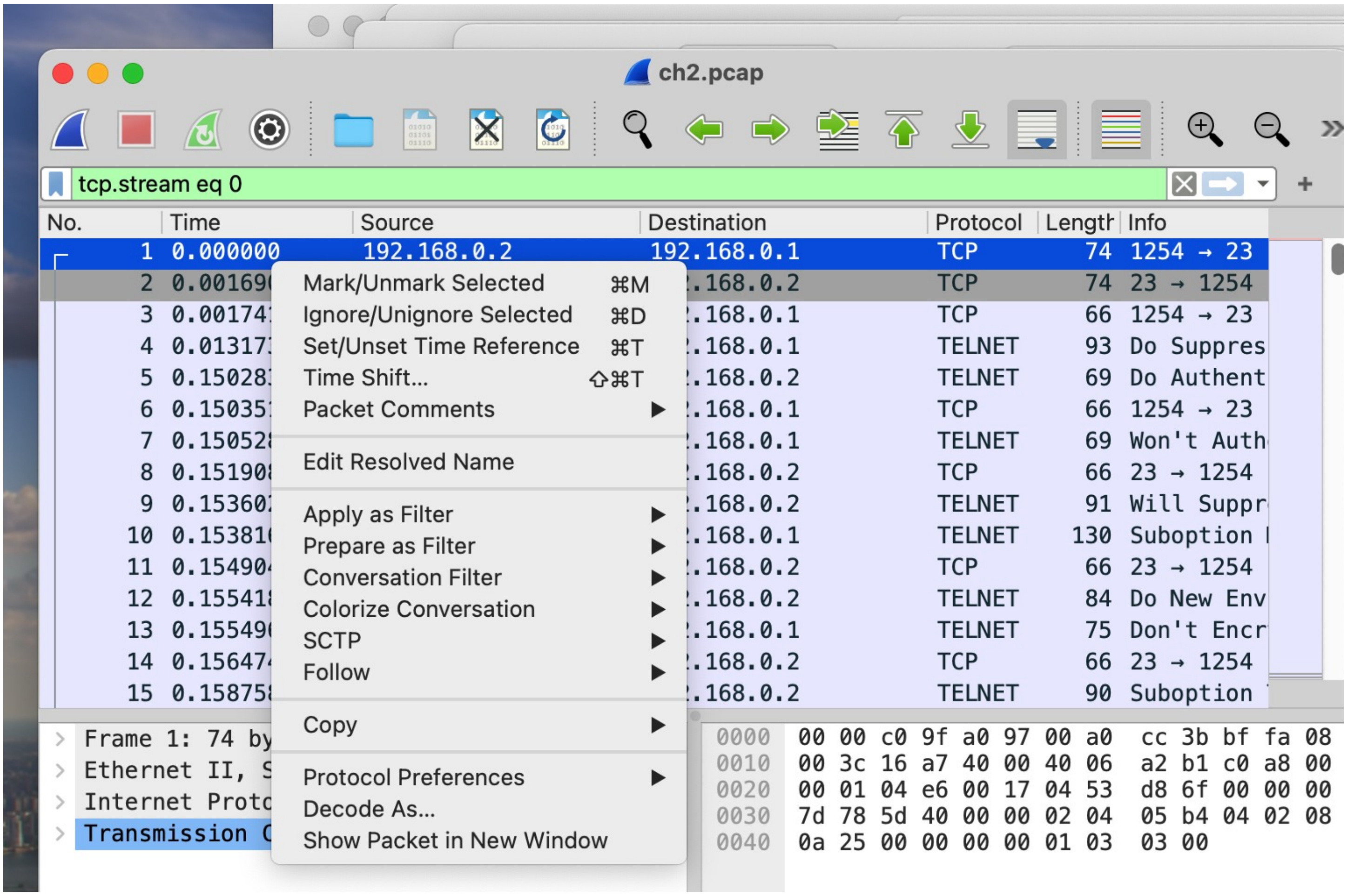
Well done, you won 10 Points

Don't forget to give your opinion on the challenge by voting ;-)

tweet it!

Enter password

2. Root me: Telnet - authentication

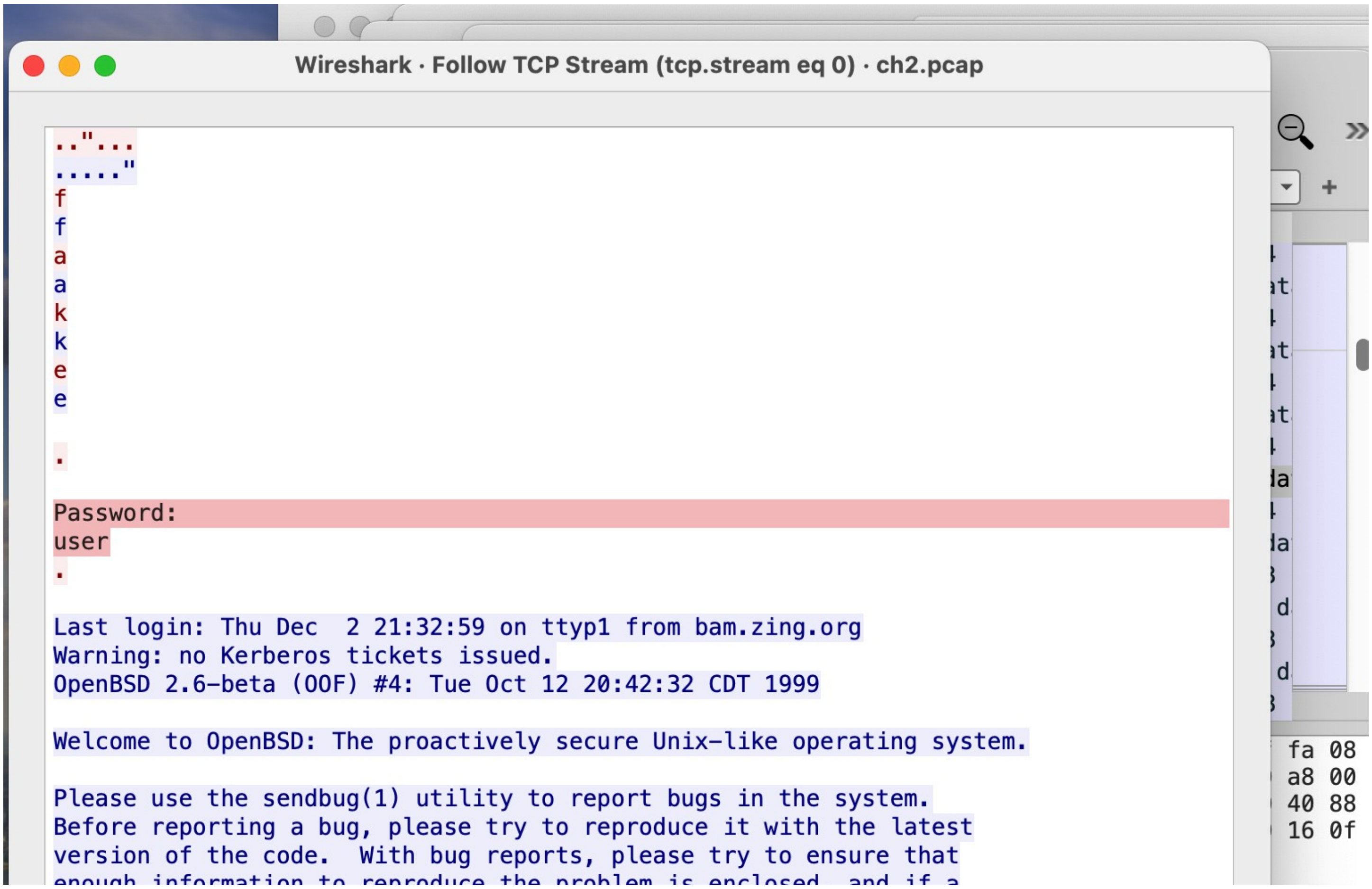


tcp.stream eq 0

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.2	192.168.0.1	TCP	74	1254 → 23
2	0.00169		.168.0.2	TCP	74	23 → 1254
3	0.00174		.168.0.1	TCP	66	1254 → 23
4	0.01317		.168.0.1	TELNET	93	Do Suppres
5	0.15028		.168.0.2	TELNET	69	Do Authent
6	0.15035		.168.0.1	TCP	66	1254 → 23
7	0.15052		.168.0.1	TELNET	69	Won't Auth
8	0.15190		.168.0.2	TCP	66	23 → 1254
9	0.15360		.168.0.2	TELNET	91	Will Suppr
10	0.15381		.168.0.1	TELNET	130	Suboption
11	0.15490		.168.0.2	TCP	66	23 → 1254
12	0.15541		.168.0.2	TELNET	84	Do New Env
13	0.15549		.168.0.1	TELNET	75	Don't Encr
14	0.15647		.168.0.2	TCP	66	23 → 1254
15	0.15875		.168.0.2	TELNET	90	Suboption

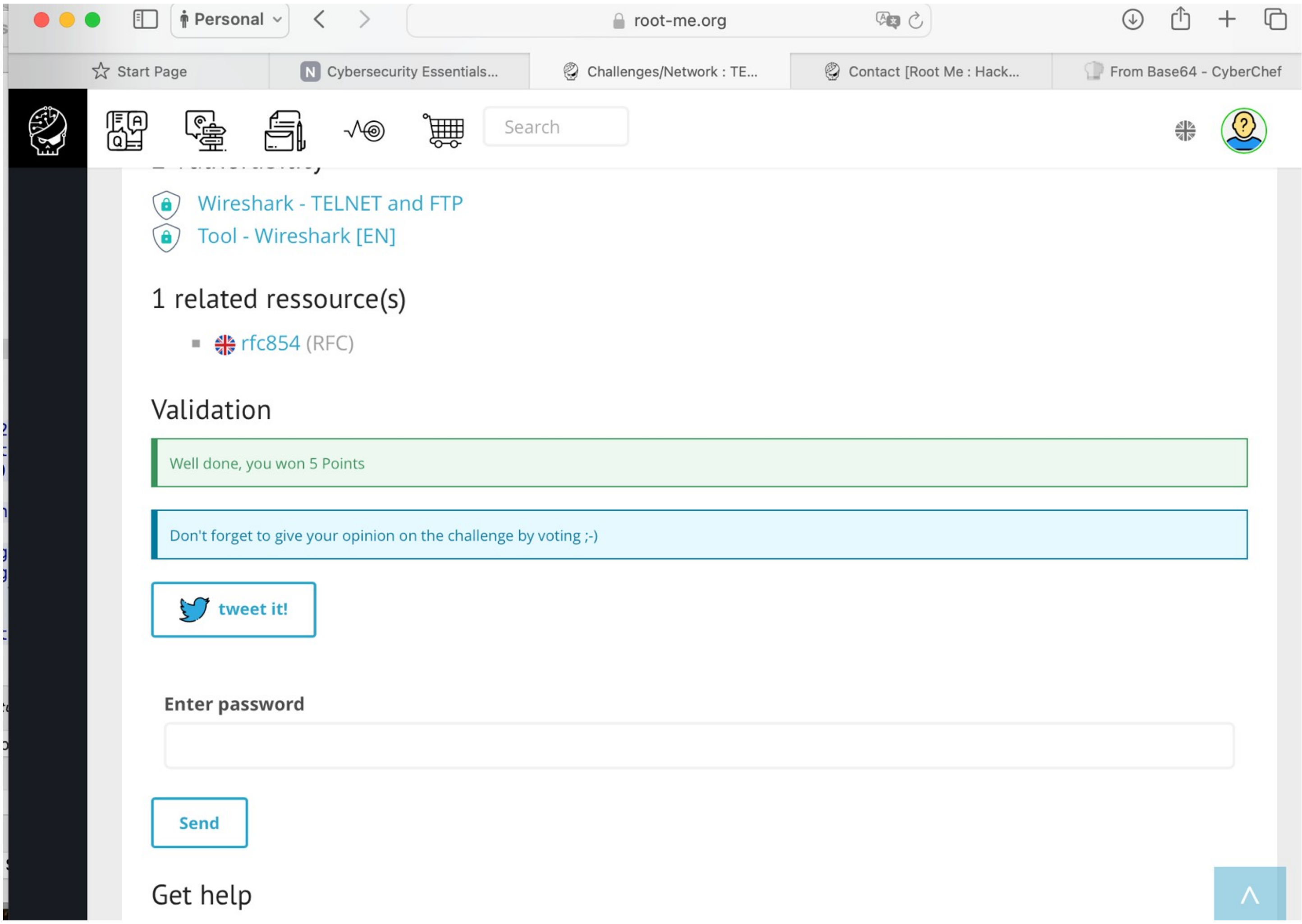
```
> Frame 1: 74 by
> Ethernet II, S
> Internet Proto
> Transmission C
```

```
0000  00 00 c0 9f a0 97 00 a0  cc 3b bf fa 08
0010  00 3c 16 a7 40 00 40 06  a2 b1 c0 a8 00
0020  00 01 04 e6 00 17 04 53  d8 6f 00 00 00
0030  7d 78 5d 40 00 00 02 04  05 b4 04 02 08
0040  0a 25 00 00 00 00 01 03  03 00
```



Wireshark · Follow TCP Stream (tcp.stream eq 0) · ch2.pcap

```
.."...
....."
f
f
a
a
k
k
e
e

.

Password:
user
.

Last login: Thu Dec  2 21:32:59 on ttyp1 from bam.zing.org
Warning: no Kerberos tickets issued.
OpenBSD 2.6-beta (OOF) #4: Tue Oct 12 20:42:32 CDT 1999

Welcome to OpenBSD: The proactively secure Unix-like operating system.

Please use the sendbug(1) utility to report bugs in the system.
Before reporting a bug, please try to reproduce it with the latest
version of the code.  With bug reports, please try to ensure that
enough information to reproduce the problem is enclosed, and if a
```


Personal
root-me.org
Start Page
Cybersecurity Essentials...
Challenges/Network : TE...
Contact [Root Me : Hack...
From Base64 - CyberChef
Search

Wireshark - TELNET and FTP

Tool - Wireshark [EN]

1 related ressource(s)

- rfc854 (RFC)

Validation

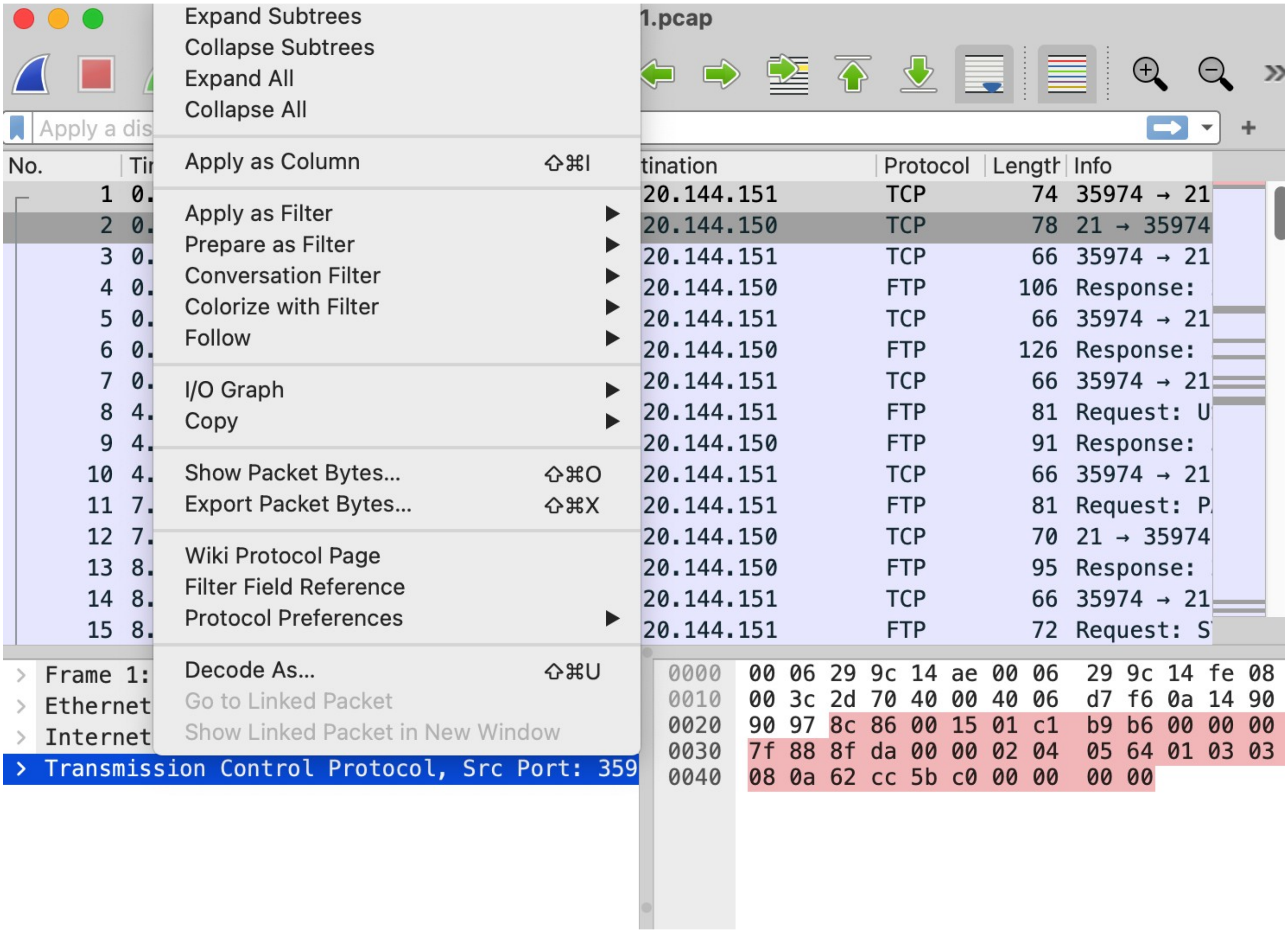
Well done, you won 5 Points

Don't forget to give your opinion on the challenge by voting ;-)

Enter password

Get help

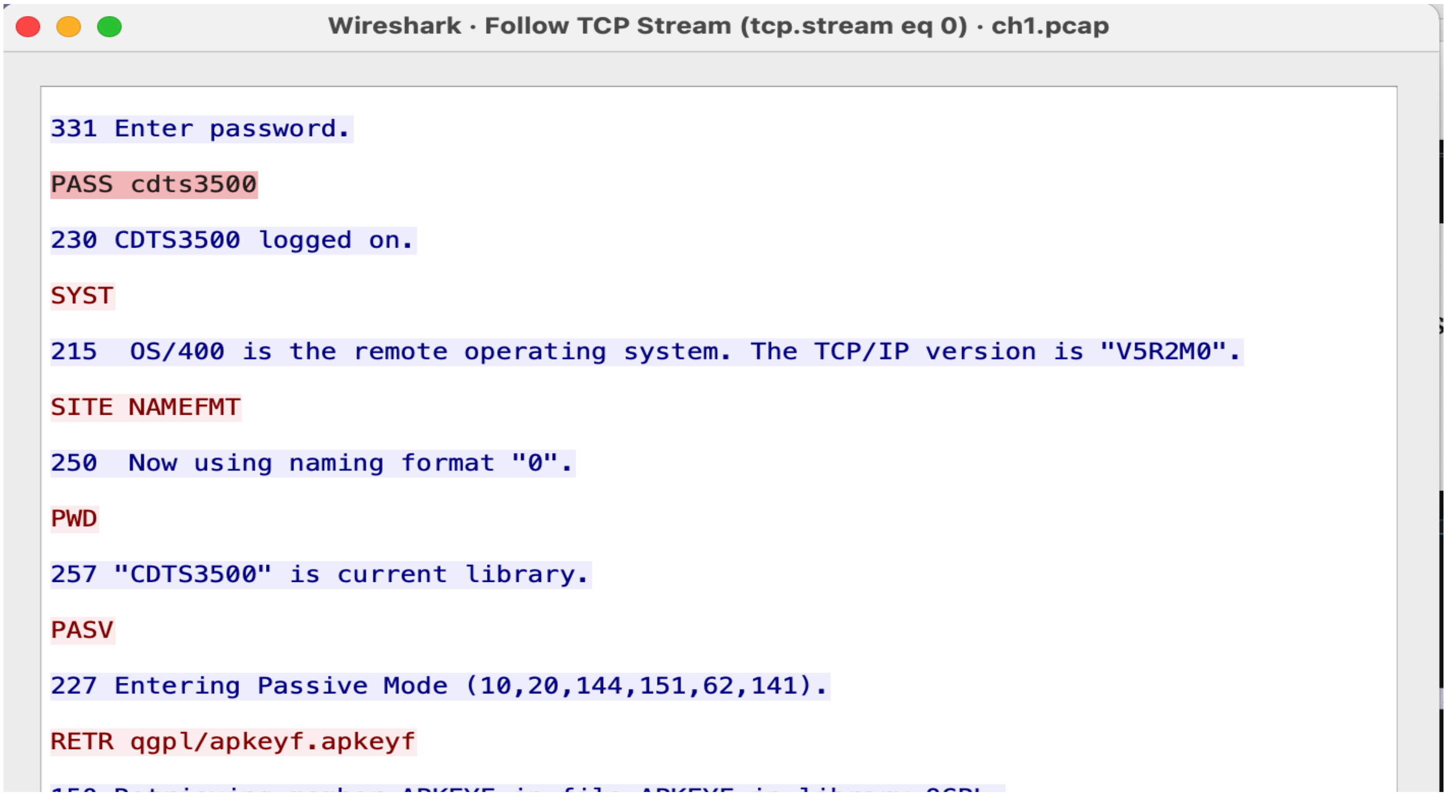
3. Root me: Ftp - authentication



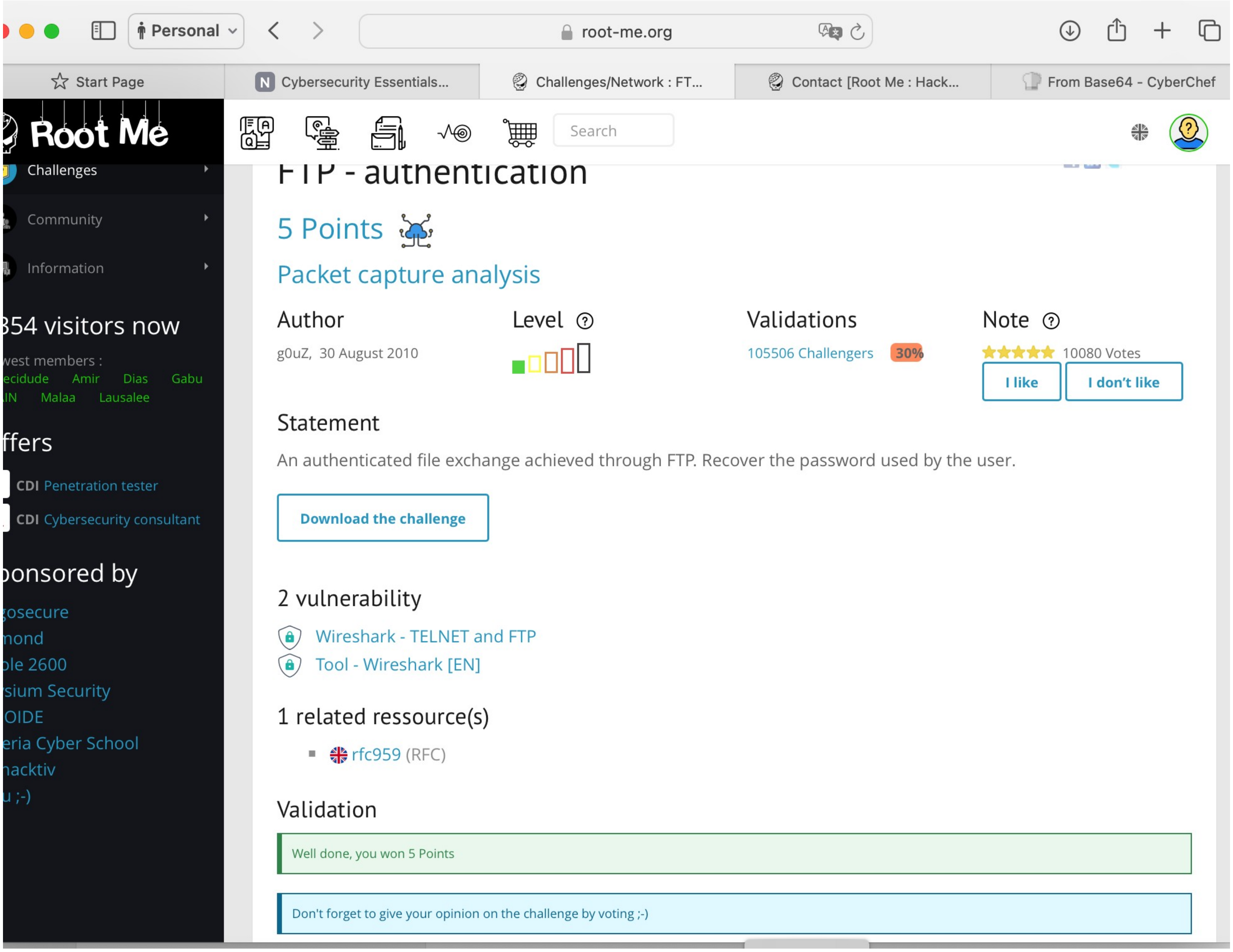
```
No.  Ti   tination     Protocol  Length  Info
  1  0.   20.144.151   TCP       74      35974 → 21
  2  0.   20.144.150   TCP       78      21 → 35974
  3  0.   20.144.151   TCP       66      35974 → 21
  4  0.   20.144.150   FTP       106     Response:
  5  0.   20.144.151   TCP       66      35974 → 21
  6  0.   20.144.150   FTP       126     Response:
  7  0.   20.144.151   TCP       66      35974 → 21
  8  4.   20.144.151   FTP       81      Request: U
  9  4.   20.144.150   FTP       91      Response:
 10  4.   20.144.151   TCP       66      35974 → 21
 11  7.   20.144.151   FTP       81      Request: P
 12  7.   20.144.150   TCP       70      21 → 35974
 13  8.   20.144.150   FTP       95      Response:
 14  8.   20.144.151   TCP       66      35974 → 21
 15  8.   20.144.151   FTP       72      Request: S
```

```
> Frame 1:
> Ethernet
> Internet
> Transmission Control Protocol, Src Port: 359
```

```
0000  00 06 29 9c 14 ae 00 06  29 9c 14 fe 08
0010  00 3c 2d 70 40 00 40 06  d7 f6 0a 14 90
0020  90 97 8c 86 00 15 01 c1  b9 b6 00 00 00
0030  7f 88 8f da 00 00 02 04  05 64 01 03 03
0040  08 0a 62 cc 5b c0 00 00  00 00
```



```
331 Enter password.

PASS cdts3500

230 CDTS3500 logged on.

SYST

215  OS/400 is the remote operating system. The TCP/IP version is "V5R2M0".

SITE NAMEFMT

250  Now using naming format "0".

PWD

257 "CDTS3500" is current library.

PASV

227 Entering Passive Mode (10,20,144,151,62,141).

RETR qgpl/apkeyf.apkeyf

150 Retrieving member APKEYF in file APKEYF in library QGPL.
```



FTP - authentication

5 Points

Packet capture analysis

Author	Level	Validations	Note
g0uZ, 30 August 2010		105506 Challengers 30%	★★★★★ 10080 Votes

Statement

An authenticated file exchange achieved through FTP. Recover the password used by the user.

2 vulnerability

- Wireshark - TELNET and FTP
- Tool - Wireshark [EN]

1 related ressource(s)

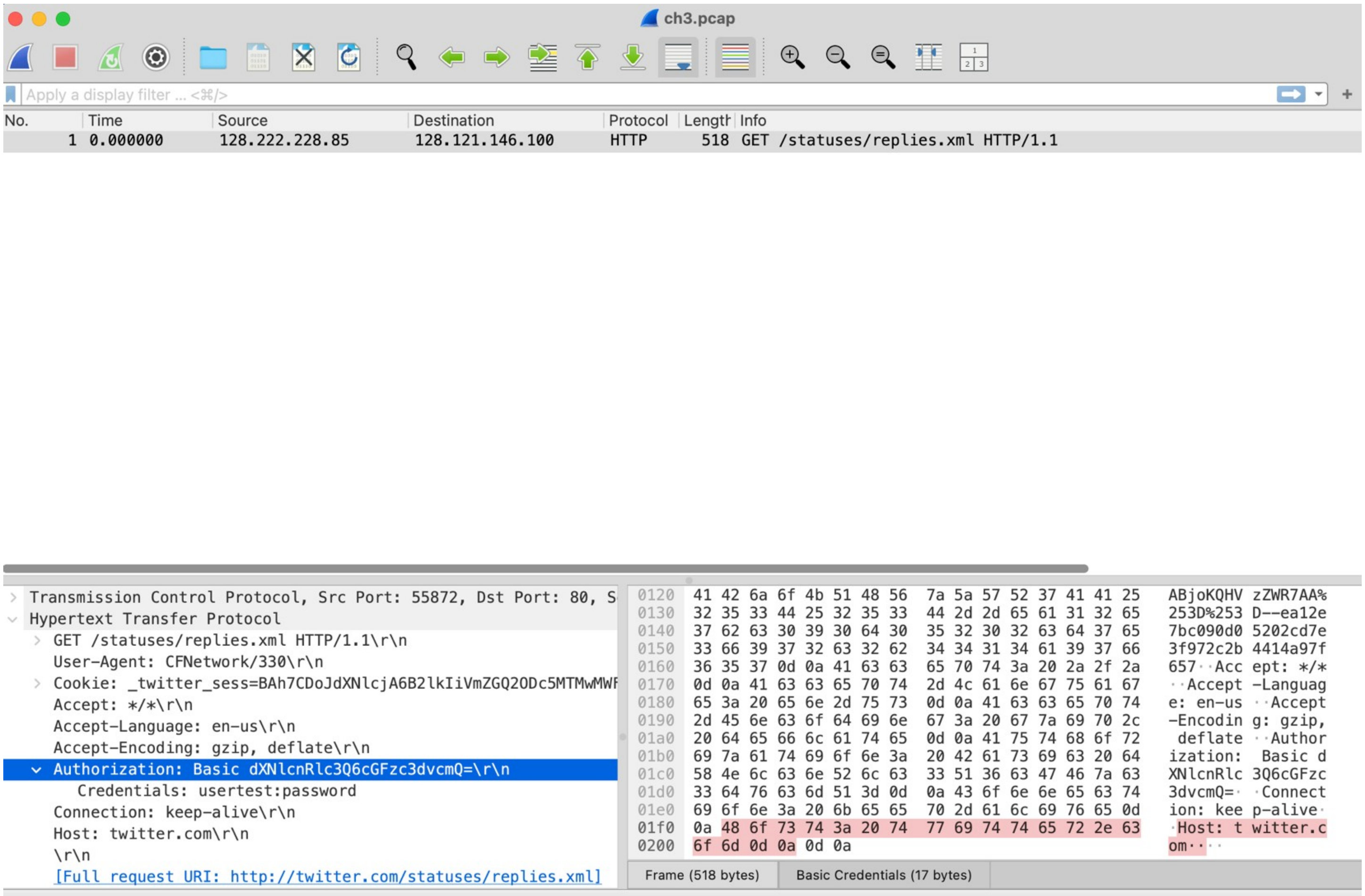
- rfc959 (RFC)

Validation

Well done, you won 5 Points

Don't forget to give your opinion on the challenge by voting ;-)

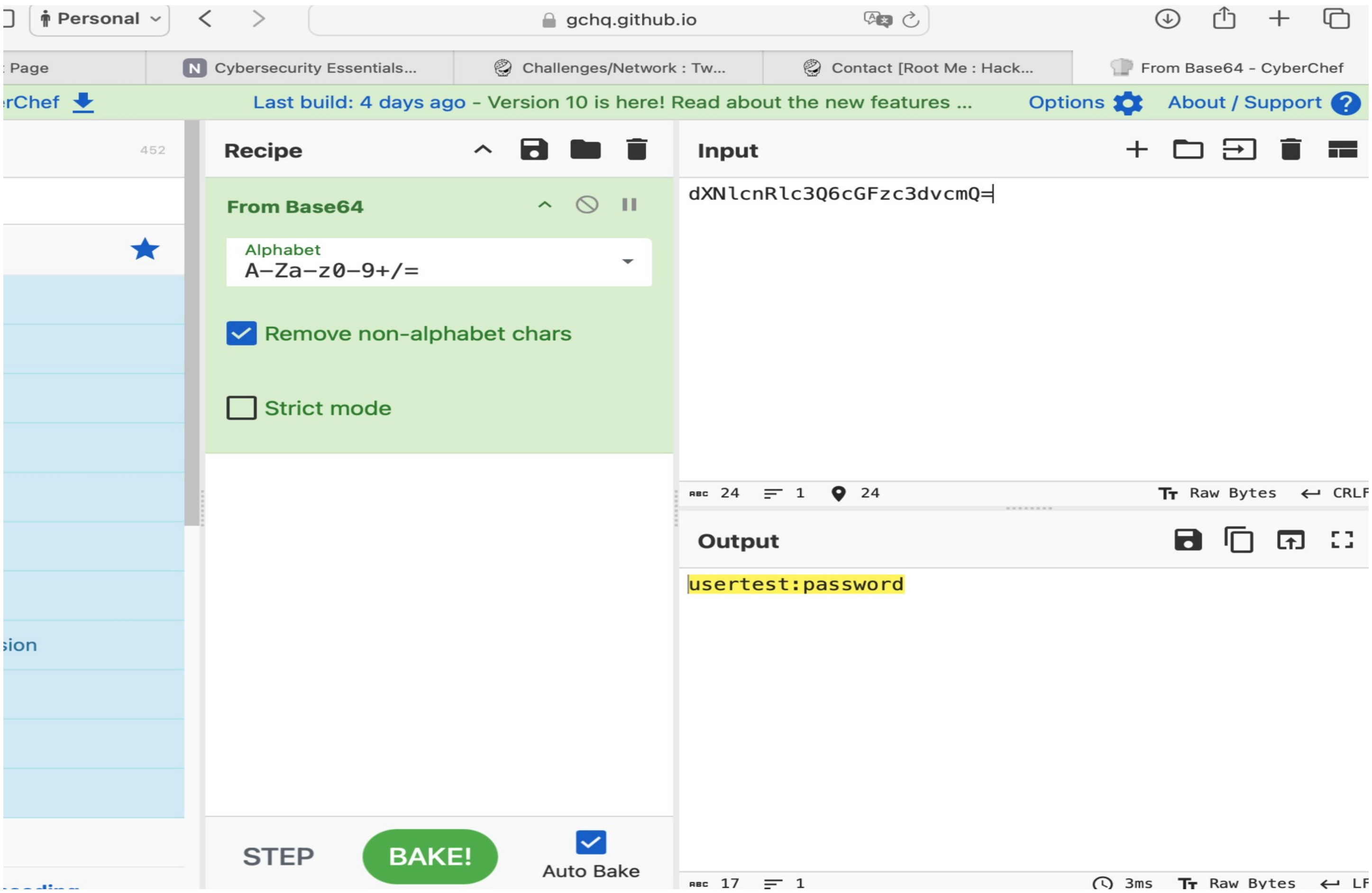
4. Root me: Twitter authentication



```
No.   Time      Source          Destination      Protocol Length Info
    1 0.000000  128.222.228.85  128.121.146.100  HTTP      518  GET /statuses/replies.xml HTTP/1.1
```

```
> Transmission Control Protocol, Src Port: 55872, Dst Port: 80, S
v Hypertext Transfer Protocol
  > GET /statuses/replies.xml HTTP/1.1\r\n
    User-Agent: CFNetwork/330\r\n
  > Cookie: _twitter_sess=BAh7CDoJdXNlcjA6B2lkIiVmZGQ2ODc5MTMwMWF
    Accept: */*\r\n
    Accept-Language: en-us\r\n
    Accept-Encoding: gzip, deflate\r\n
  v Authorization: Basic dXNlcnRlc3Q6cGFzc3dvcmQ=\r\n
      Credentials: usertest:password
    Connection: keep-alive\r\n
    Host: twitter.com\r\n
    \r\n
    [Full request URI: http://twitter.com/statuses/replies.xml]
```

```
0120  41 42 6a 6f 4b 51 48 56  7a 5a 57 52 37 41 41 25   ABjoKQHV zZWR7AA%
0130  32 35 33 44 25 32 35 33  44 2d 2d 65 61 31 32 65   253D%253 D--ea12e
0140  37 62 63 30 39 30 64 30  35 32 30 32 63 64 37 65   7bc090d0 5202cd7e
0150  33 66 39 37 32 63 32 62  34 34 31 34 61 39 37 66   3f972c2b 4414a97f
0160  36 35 37 0d 0a 41 63 63  65 70 74 3a 20 2a 2f 2a   657··Acc ept: */*
0170  0d 0a 41 63 63 65 70 74  2d 4c 61 6e 67 75 61 67   ··Accept -Languag
0180  65 3a 20 65 6e 2d 75 73  0d 0a 41 63 63 65 70 74   e: en-us ··Accept
0190  2d 45 6e 63 6f 64 69 6e  67 3a 20 67 7a 69 70 2c   -Encodin g: gzip,
01a0  20 64 65 66 6c 61 74 65  0d 0a 41 75 74 68 6f 72    deflate ··Author
01b0  69 7a 61 74 69 6f 6e 3a  20 42 61 73 69 63 20 64   ization:  Basic d
01c0  58 4e 6c 63 6e 52 6c 63  33 51 36 63 47 46 7a 63   XNlcnRlc 3Q6cGFzc
01d0  33 64 76 63 6d 51 3d 0d  0a 43 6f 6e 6e 65 63 74   3dvcmQ=· ·Connect
01e0  69 6f 6e 3a 20 6b 65 65  70 2d 61 6c 69 76 65 0d   ion: kee p-alive·
01f0  0a 48 6f 73 74 3a 20 74  77 69 74 74 65 72 2e 63   ·Host: t witter.c
0200  6f 6d 0d 0a 0d 0a                                  om····
```



Personal
gchq.github.io
Page
Cybersecurity Essentials...
Challenges/Network : Tw...
Contact [Root Me : Hack...
From Base64 - CyberChef
rChef
Last build: 4 days ago - Version 10 is here! Read about the new features ...
Options
About / Support
452
sion
Recipe
Input
Output
STEP
BAKE!
Auto Bake

From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars

☐ Strict mode

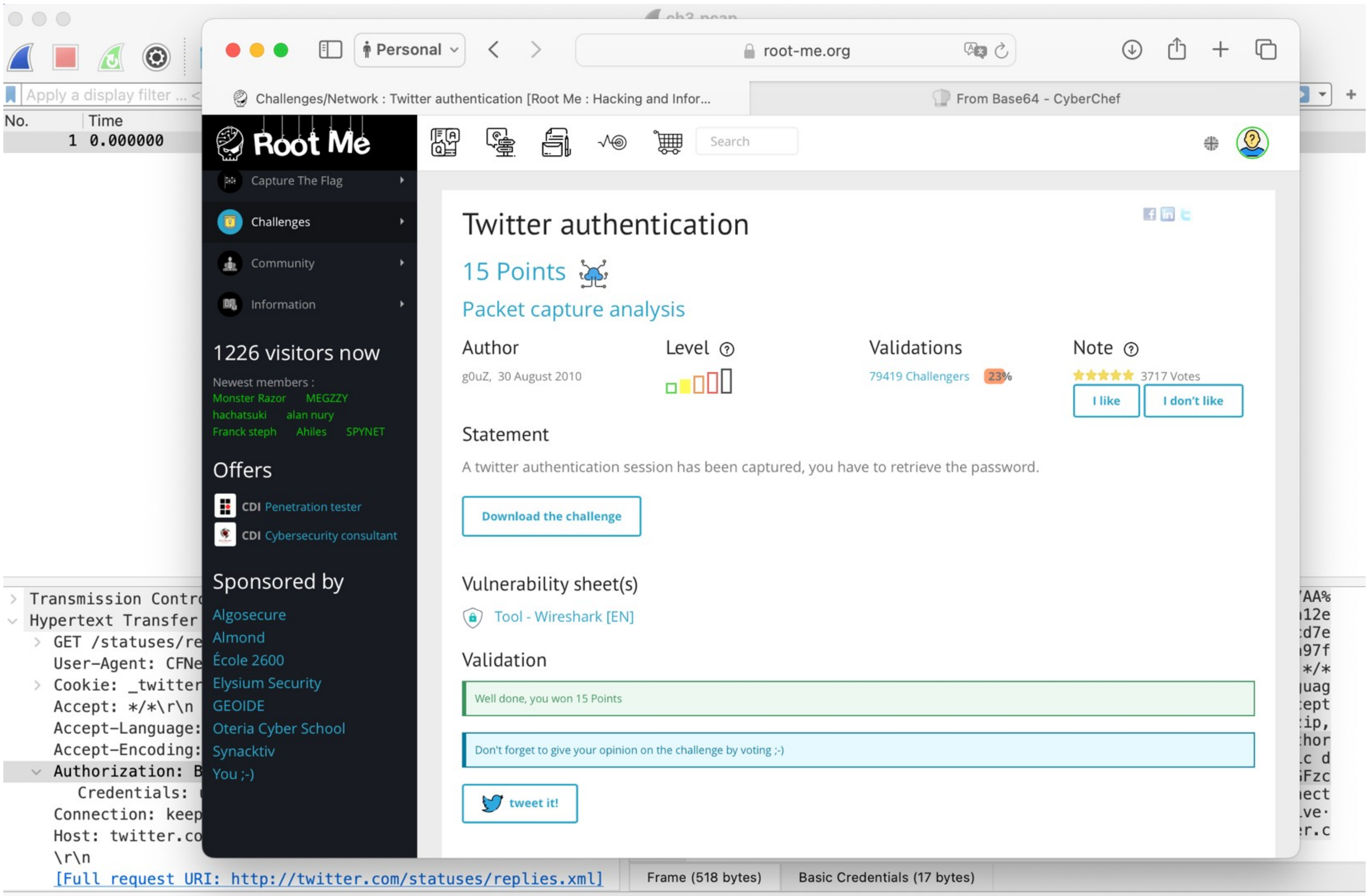
☑ Auto Bake

```
dXNlcnRlc3Q6cGFzc3dvcmQ=
```

abc 24 1 24 Raw Bytes CRLF

```
usertest:password
```

abc 17 1 3ms Raw Bytes LF



```
No.     Time
  1 0.000000

> Transmission Contr
v Hypertext Transfer
  > GET /statuses/re
    User-Agent: CFNe
  > Cookie: _twitter
    Accept: */*\r\n
    Accept-Language:
    Accept-Encoding:
  v Authorization: B
      Credentials:
    Connection: keep
    Host: twitter.co
    \r\n
    [Full request URI: http://twitter.com/statuses/replies.xml]
```

Challenges/Network : Twitter authentication [Root Me : Hacking and Infor...

From Base64 - CyberChef

Capture The Flag
Challenges
Community
Information

1226 visitors now

Newest members :
Monster Razor MEGZZY
hachatsuki alan nury
Franck steph Ahiles SPYNET

Offers

CDI Penetration tester
CDI Cybersecurity consultant

Sponsored by

Algosecure
Almond
École 2600
Elysium Security
GEOIDE
Oteria Cyber School
Synacktiv
You ;-)

Twitter authentication

15 Points

Packet capture analysis

Author	Level	Validations	Note
g0uZ, 30 August 2010		79419 Challengers 23%	★★★★★ 3717 Votes I like I don't like

Statement

A twitter authentication session has been captured, you have to retrieve the password.

Download the challenge

Vulnerability sheet(s)

Tool - Wireshark [EN]

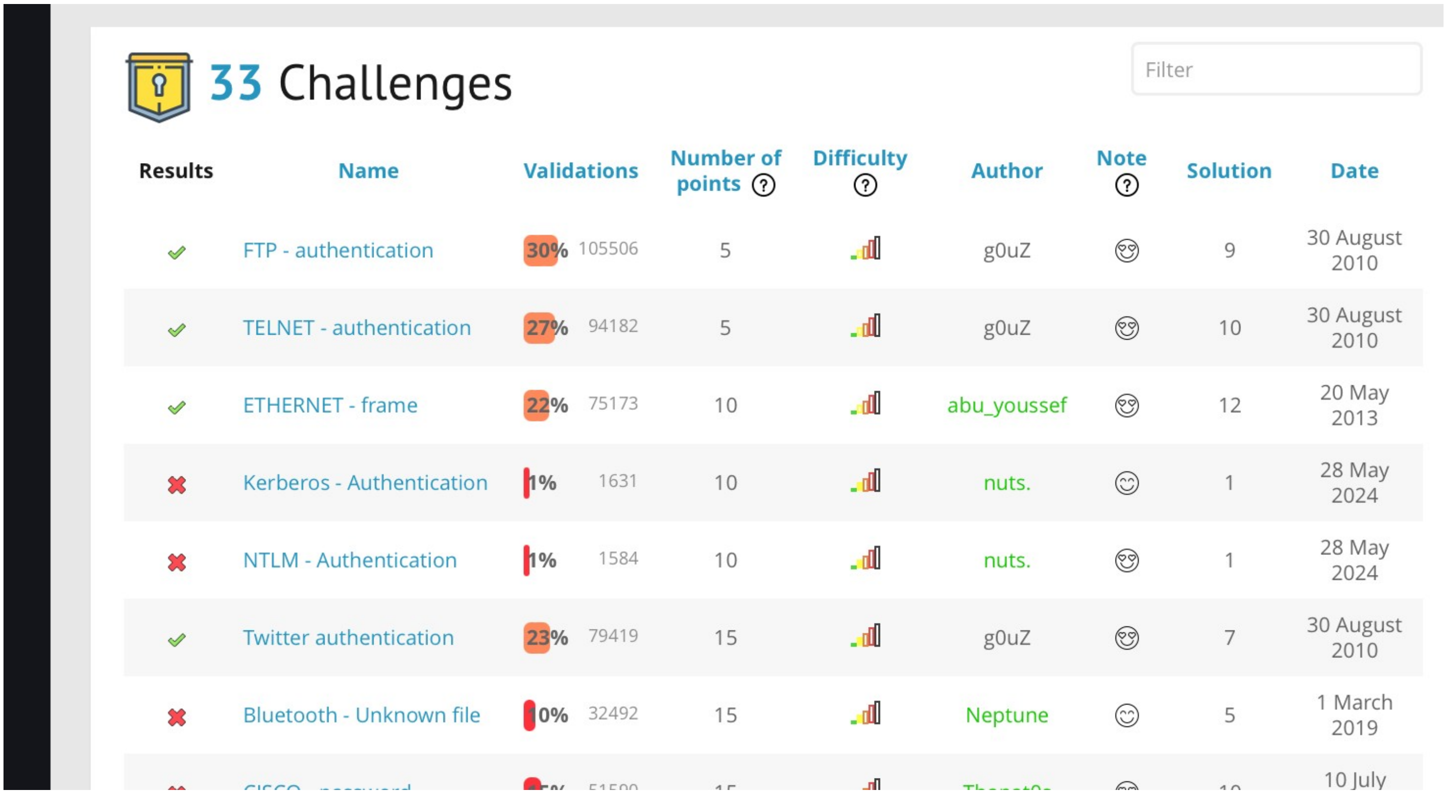
Validation

Well done, you won 15 Points

Don't forget to give your opinion on the challenge by voting ;-)

tweet it!

All completed root me challenges:

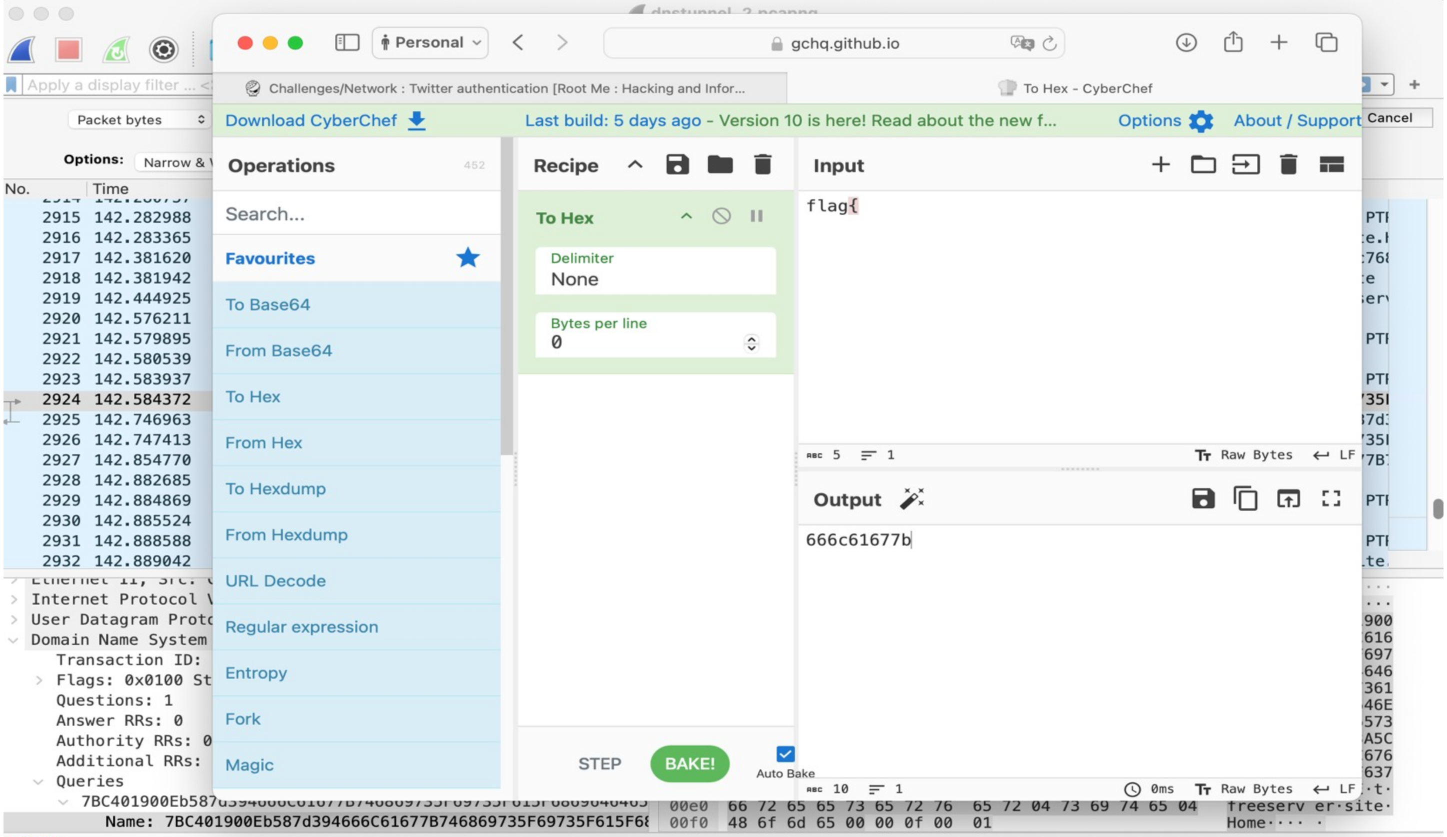


33 Challenges

Filter

Results	Name	Validations	Number of points	Difficulty	Author	Note	Solution	Date
✓	FTP - authentication	30% 105506	5		g0uZ	☺	9	30 August 2010
✓	TELNET - authentication	27% 94182	5		g0uZ	☺	10	30 August 2010
✓	ETHERNET - frame	22% 75173	10		abu_youssef	☺	12	20 May 2013
✗	Kerberos - Authentication	1% 1631	10		nuts.	☺	1	28 May 2024
✗	NTLM - Authentication	1% 1584	10		nuts.	☺	1	28 May 2024
✓	Twitter authentication	23% 79419	15		g0uZ	☺	7	30 August 2010
✗	Bluetooth - Unknown file	10% 32492	15		Neptune	☺	5	1 March 2019
✗	CISCO - password	5% 51590	15		Thanat0s	☺	10	10 July

5. DNS tunnel



To Hex

Delimiter
None

Bytes per line
0

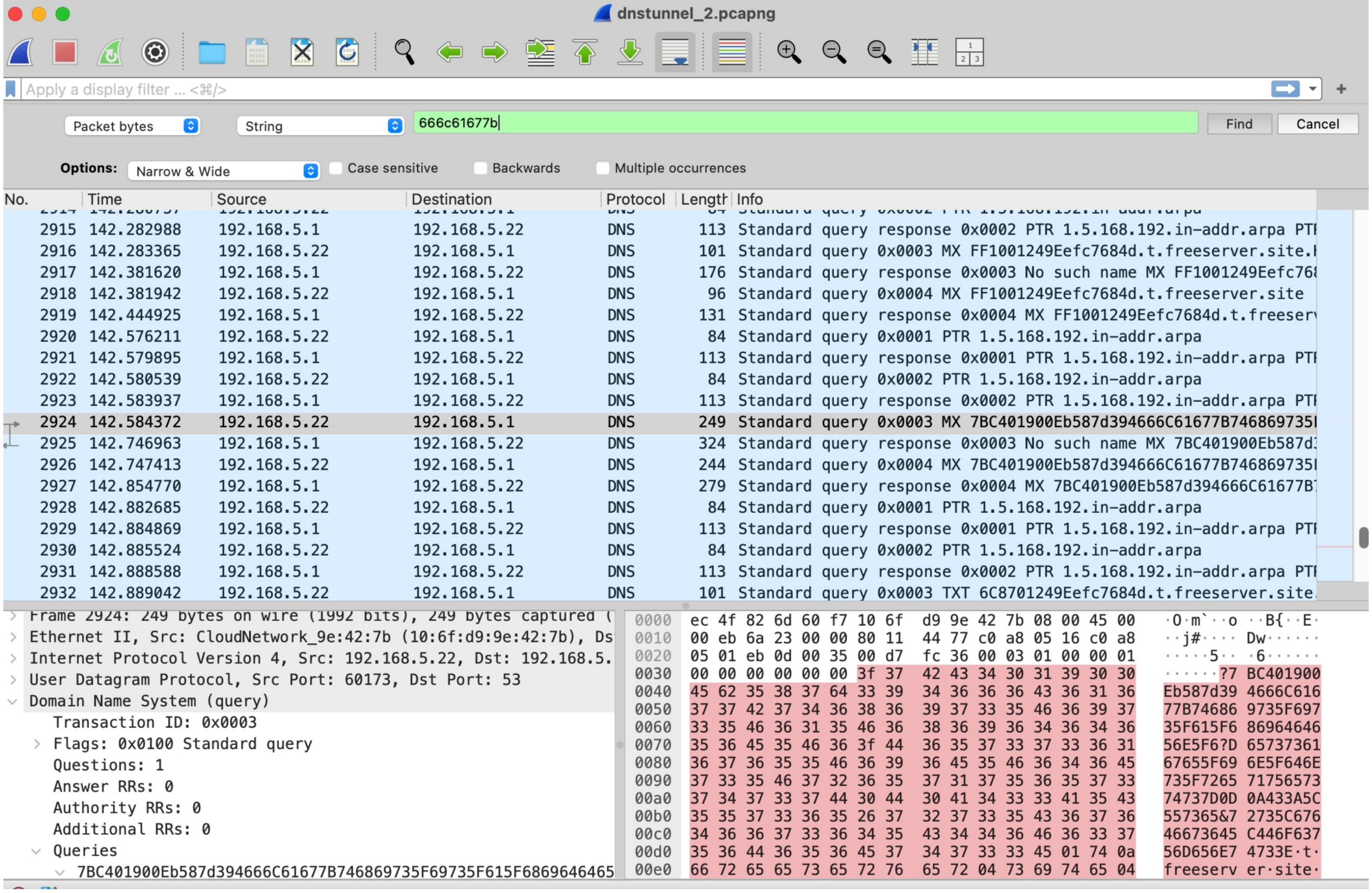
```
flag{
```

abc 5 ≡ 1

```
666c61677b
```

abc 10 ≡ 1 0ms

```
2915 142.282988
2916 142.283365
2917 142.381620
2918 142.381942
2919 142.444925
2920 142.576211
2921 142.579895
2922 142.580539
2923 142.583937
2924 142.584372
2925 142.746963
2926 142.747413
2927 142.854770
2928 142.882685
2929 142.884869
2930 142.885524
2931 142.888588
2932 142.889042
> Internet Protocol V
> User Datagram Proto
v Domain Name System
    Transaction ID:
  > Flags: 0x0100 St
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs:
  v Queries
    v 7BC401900Eb587d394666C61677B746869735F69735F615F68
        Name: 7BC401900Eb587d394666C61677B746869735F69735F615F68
00e0  66 72 65 65 73 65 72 76  65 72 04 73 69 74 65 04   freeserv er·site·
00f0  48 6f 6d 65 00 00 0f 00  01                        Home····  ·
```



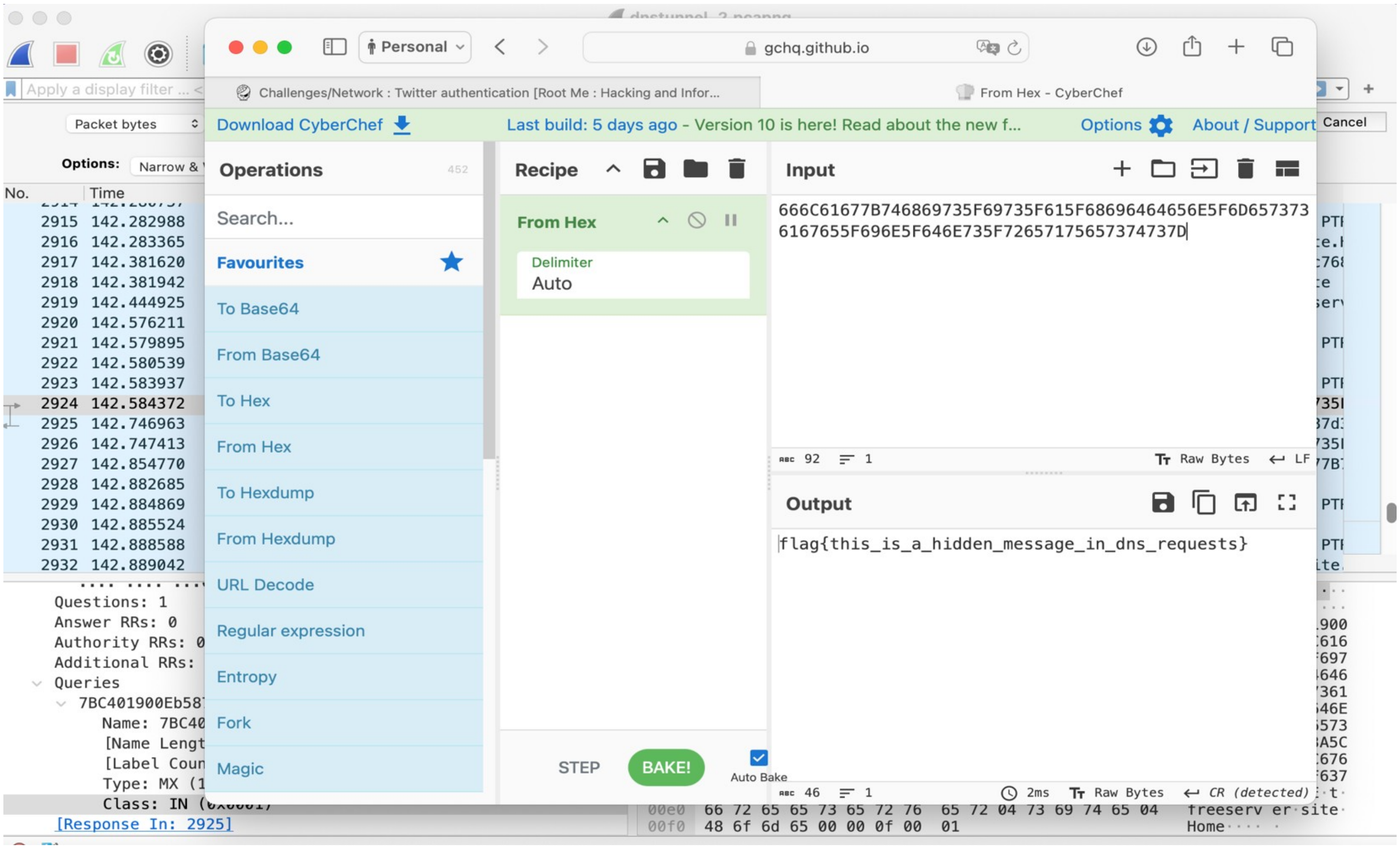
Packet bytes · String · 666c61677b

Options: Narrow & Wide · □ Case sensitive · □ Backwards · □ Multiple occurrences

```
No.   Time        Source          Destination     Protocol Length Info
2915 142.282988  192.168.5.1     192.168.5.22    DNS   113 Standard query response 0x0002 PTR 1.5.168.192.in-addr.arpa PTR
2916 142.283365  192.168.5.22    192.168.5.1     DNS   101 Standard query 0x0003 MX FF1001249Eefc7684d.t.freeserver.site.H
2917 142.381620  192.168.5.1     192.168.5.22    DNS   176 Standard query response 0x0003 No such name MX FF1001249Eefc768
2918 142.381942  192.168.5.22    192.168.5.1     DNS    96 Standard query 0x0004 MX FF1001249Eefc7684d.t.freeserver.site
2919 142.444925  192.168.5.1     192.168.5.22    DNS   131 Standard query response 0x0004 MX FF1001249Eefc7684d.t.freeserv
2920 142.576211  192.168.5.22    192.168.5.1     DNS    84 Standard query 0x0001 PTR 1.5.168.192.in-addr.arpa
2921 142.579895  192.168.5.1     192.168.5.22    DNS   113 Standard query response 0x0001 PTR 1.5.168.192.in-addr.arpa PTR
2922 142.580539  192.168.5.22    192.168.5.1     DNS    84 Standard query 0x0002 PTR 1.5.168.192.in-addr.arpa
2923 142.583937  192.168.5.1     192.168.5.22    DNS   113 Standard query response 0x0002 PTR 1.5.168.192.in-addr.arpa PTR
2924 142.584372  192.168.5.22    192.168.5.1     DNS   249 Standard query 0x0003 MX 7BC401900Eb587d394666C61677B746869735
2925 142.746963  192.168.5.1     192.168.5.22    DNS   324 Standard query response 0x0003 No such name MX 7BC401900Eb587d3
2926 142.747413  192.168.5.22    192.168.5.1     DNS   244 Standard query 0x0004 MX 7BC401900Eb587d394666C61677B746869735
2927 142.854770  192.168.5.1     192.168.5.22    DNS   279 Standard query response 0x0004 MX 7BC401900Eb587d394666C61677B7
2928 142.882685  192.168.5.22    192.168.5.1     DNS    84 Standard query 0x0001 PTR 1.5.168.192.in-addr.arpa
2929 142.884869  192.168.5.1     192.168.5.22    DNS   113 Standard query response 0x0001 PTR 1.5.168.192.in-addr.arpa PTR
2930 142.885524  192.168.5.22    192.168.5.1     DNS    84 Standard query 0x0002 PTR 1.5.168.192.in-addr.arpa
2931 142.888588  192.168.5.1     192.168.5.22    DNS   113 Standard query response 0x0002 PTR 1.5.168.192.in-addr.arpa PTR
2932 142.889042  192.168.5.22    192.168.5.1     DNS   101 Standard query 0x0003 TXT 6C8701249Eefc7684d.t.freeserver.site.
```

```
> Frame 2924: 249 bytes on wire (1992 bits), 249 bytes captured (
> Ethernet II, Src: CloudNetwork_9e:42:7b (10:6f:d9:9e:42:7b), Ds
> Internet Protocol Version 4, Src: 192.168.5.22, Dst: 192.168.5.
> User Datagram Protocol, Src Port: 60173, Dst Port: 53
v Domain Name System (query)
    Transaction ID: 0x0003
  > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v 7BC401900Eb587d394666C61677B746869735F69735F615F6869646465
```

```
0000  ec 4f 82 6d 60 f7 10 6f  d9 9e 42 7b 08 00 45 00   ·O·m`··o ··B{··E·
0010  00 eb 6a 23 00 00 80 11  44 77 c0 a8 05 16 c0 a8   ··j#···· Dw······
0020  05 01 eb 0d 00 35 00 d7  fc 36 00 03 01 00 00 01   ·····5·· ·6······
0030  00 00 00 00 00 00 3f 37  42 43 34 30 31 39 30 30   ······?7 BC401900
0040  45 62 35 38 37 64 33 39  34 36 36 36 43 36 31 36   Eb587d39 4666C616
0050  37 37 42 37 34 36 38 36  39 37 33 35 46 36 39 37   77B74686 9735F697
0060  33 35 46 36 31 35 46 36  38 36 39 36 34 36 34 36   35F615F6 86964646
0070  35 36 45 35 46 36 3f 44  36 35 37 33 37 33 36 31   56E5F6?D 65737361
0080  36 37 36 35 35 46 36 39  36 45 35 46 36 34 36 45   67655F69 6E5F646E
0090  37 33 35 46 37 32 36 35  37 31 37 35 36 35 37 33   735F7265 71756573
00a0  37 34 37 33 37 44 30 44  30 41 34 33 33 41 35 43   74737D0D 0A433A5C
00b0  35 35 37 33 36 35 26 37  32 37 33 35 43 36 37 36   557365&7 2735C676
00c0  34 36 36 37 33 36 34 35  43 34 34 36 46 36 33 37   46673645 C446F637
00d0  35 36 44 36 35 36 45 37  34 37 33 33 45 01 74 0a   56D656E7 4733E·t·
00e0  66 72 65 65 73 65 72 76  65 72 04 73 69 74 65 04   freeserv er·site·
```



Delimiter: Auto

Input

```
666C61677B746869735F69735F615F68696464656E5F6D657373
6167655F696E5F646E735F72657175657374737D
```

Output

```
flag{this_is_a_hidden_message_in_dns_requests}
```

```
No.   Time
2915 142.282988
2916 142.283365
2917 142.381620
2918 142.381942
2919 142.444925
2920 142.576211
2921 142.579895
2922 142.580539
2923 142.583937
2924 142.584372
2925 142.746963
2926 142.747413
2927 142.854770
2928 142.882685
2929 142.884869
2930 142.885524
2931 142.888588
2932 142.889042
```

```
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs:
  Queries
    7BC401900Eb58
      Name: 7BC40
      [Name Lengt
      [Label Coun
      Type: MX (1
      Class: IN (0x0001)
  [Response In: 2925]
```

```
00e0  66 72 65 65 73 65 72 76  65 72 04 73 69 74 65 04   freeserv er·site·
00f0  48 6f 6d 65 00 00 0f 00  01                        Home····  ·
```