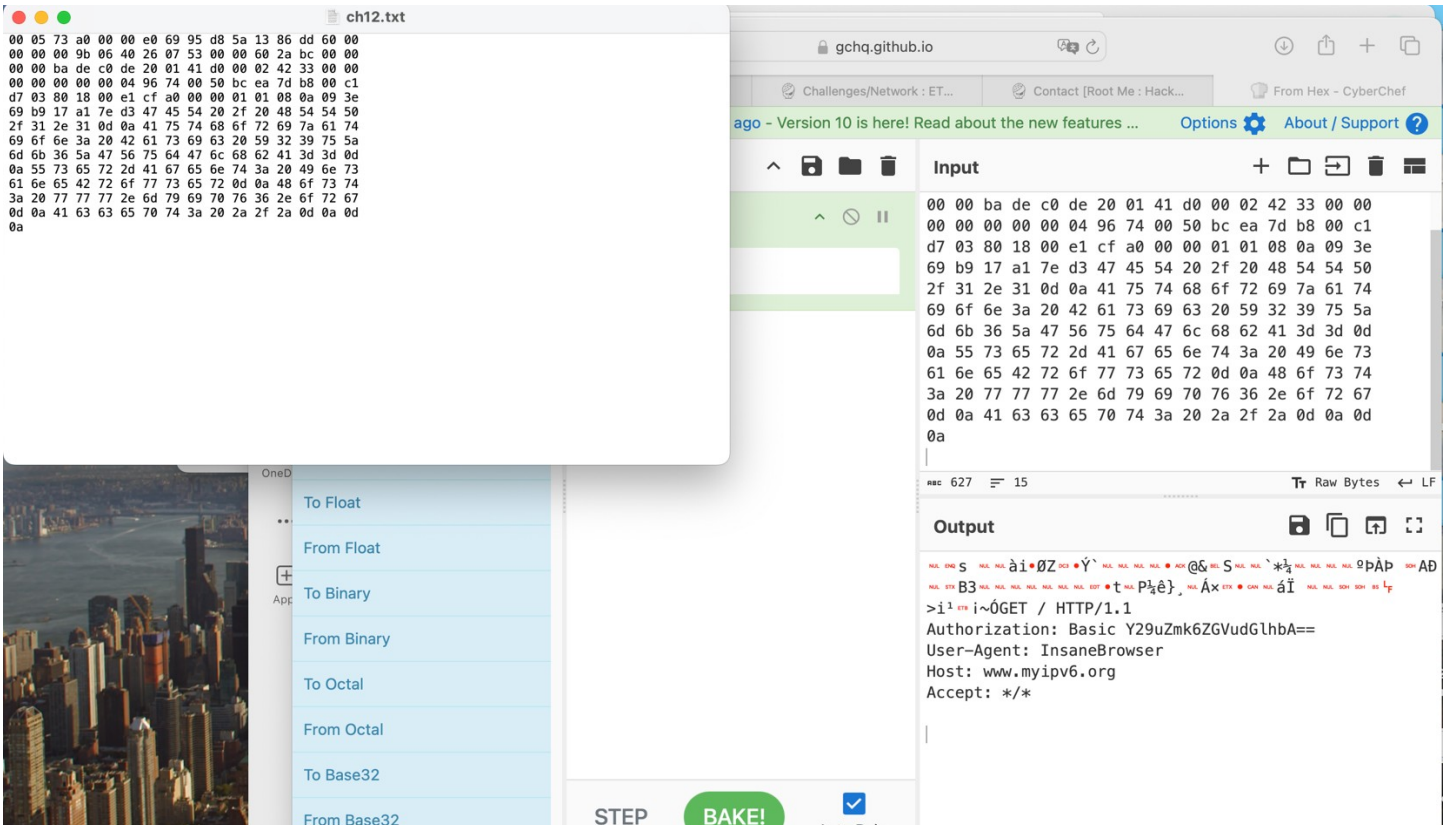
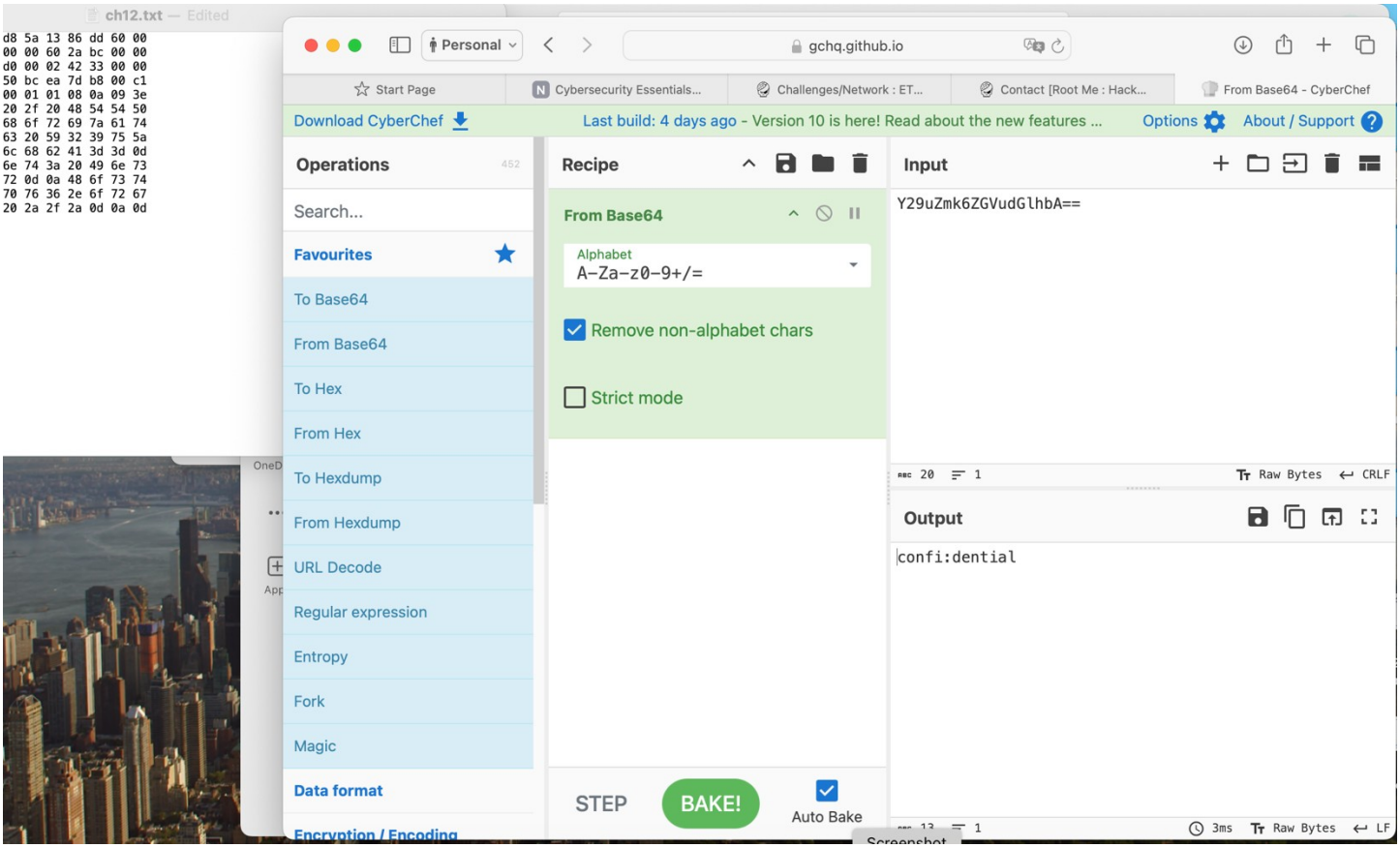
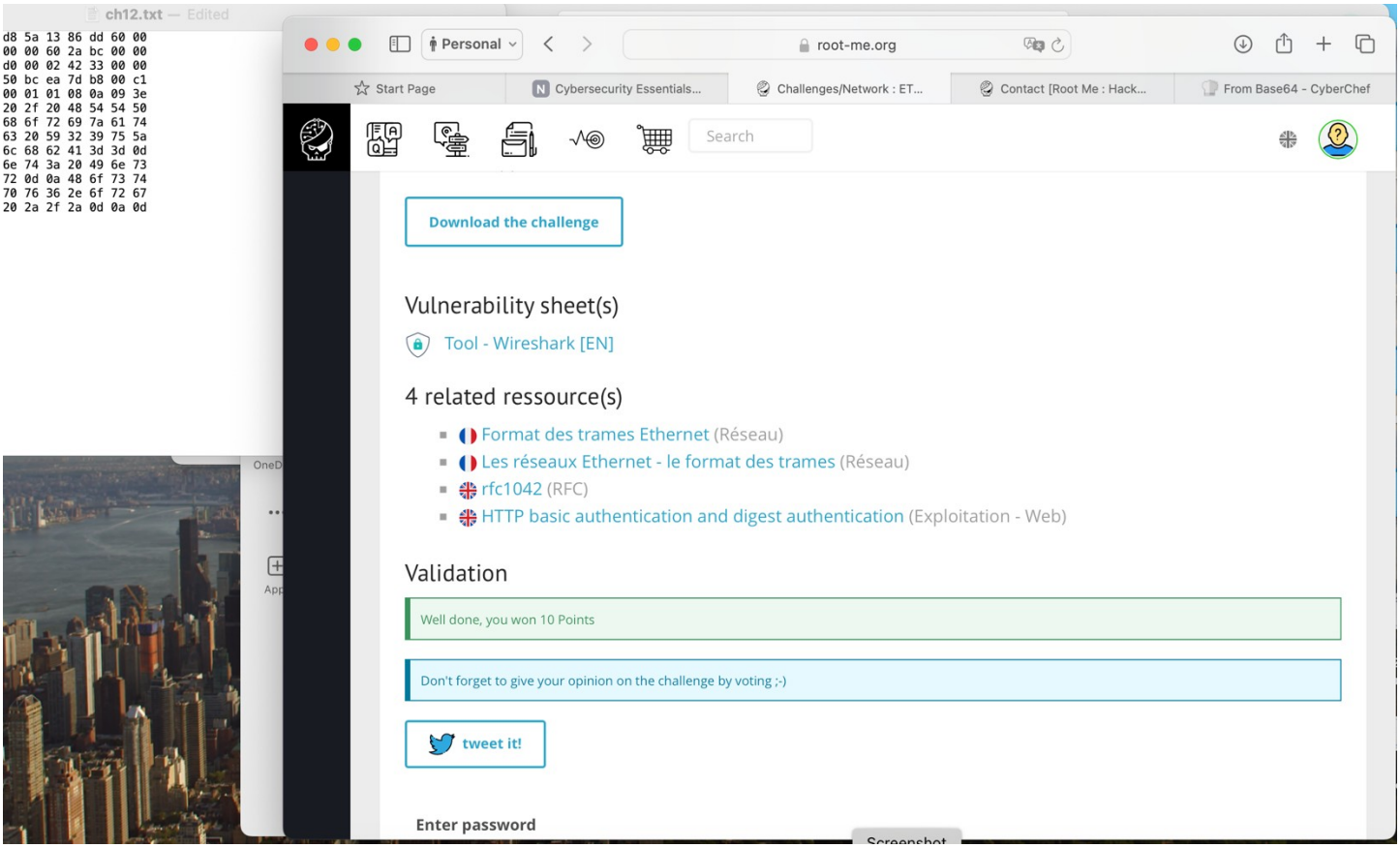
TSIS 5

Completed by Gaaze Verena, 22B030332

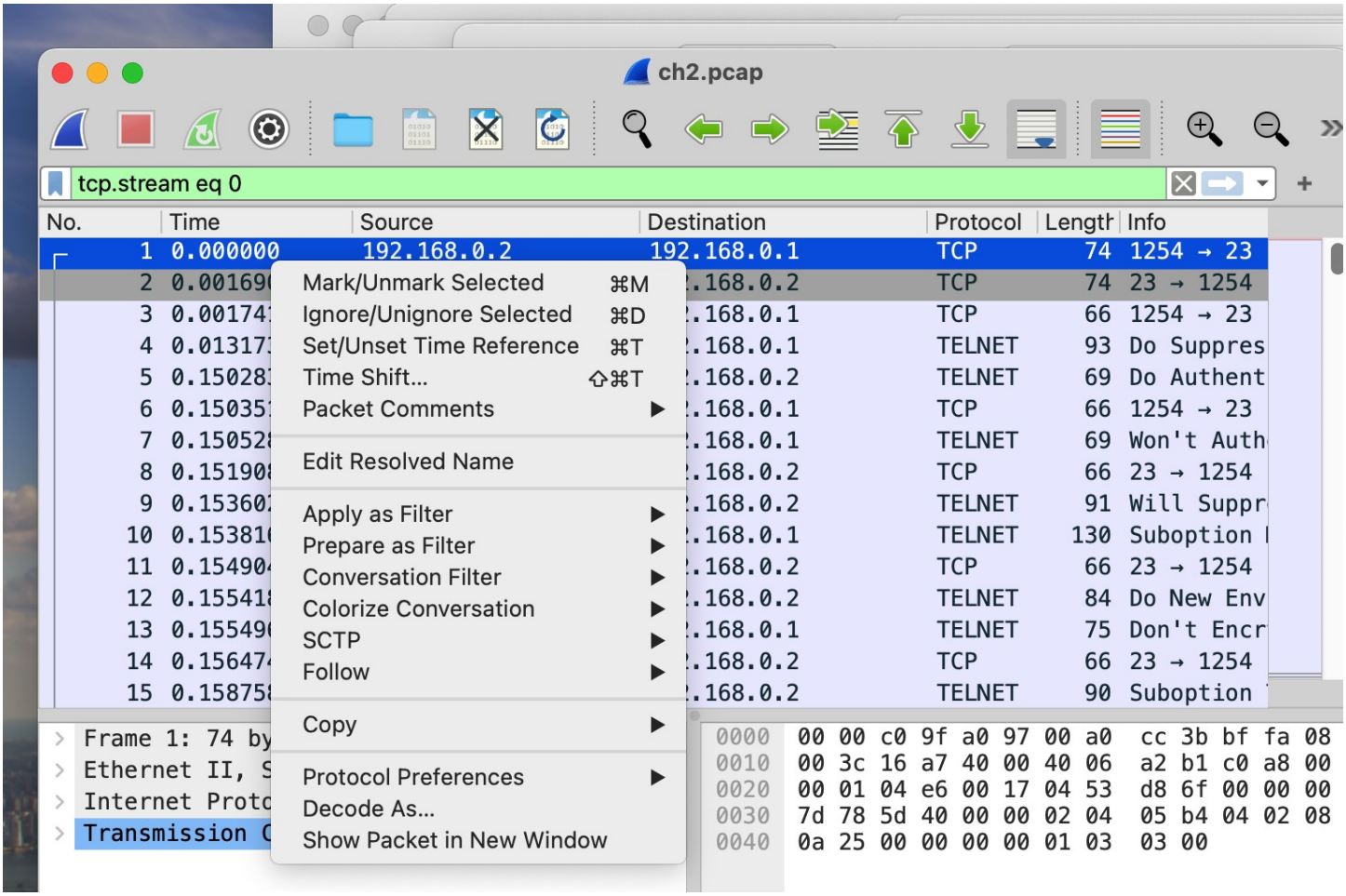
1. **Root me: Ethernet -frame**

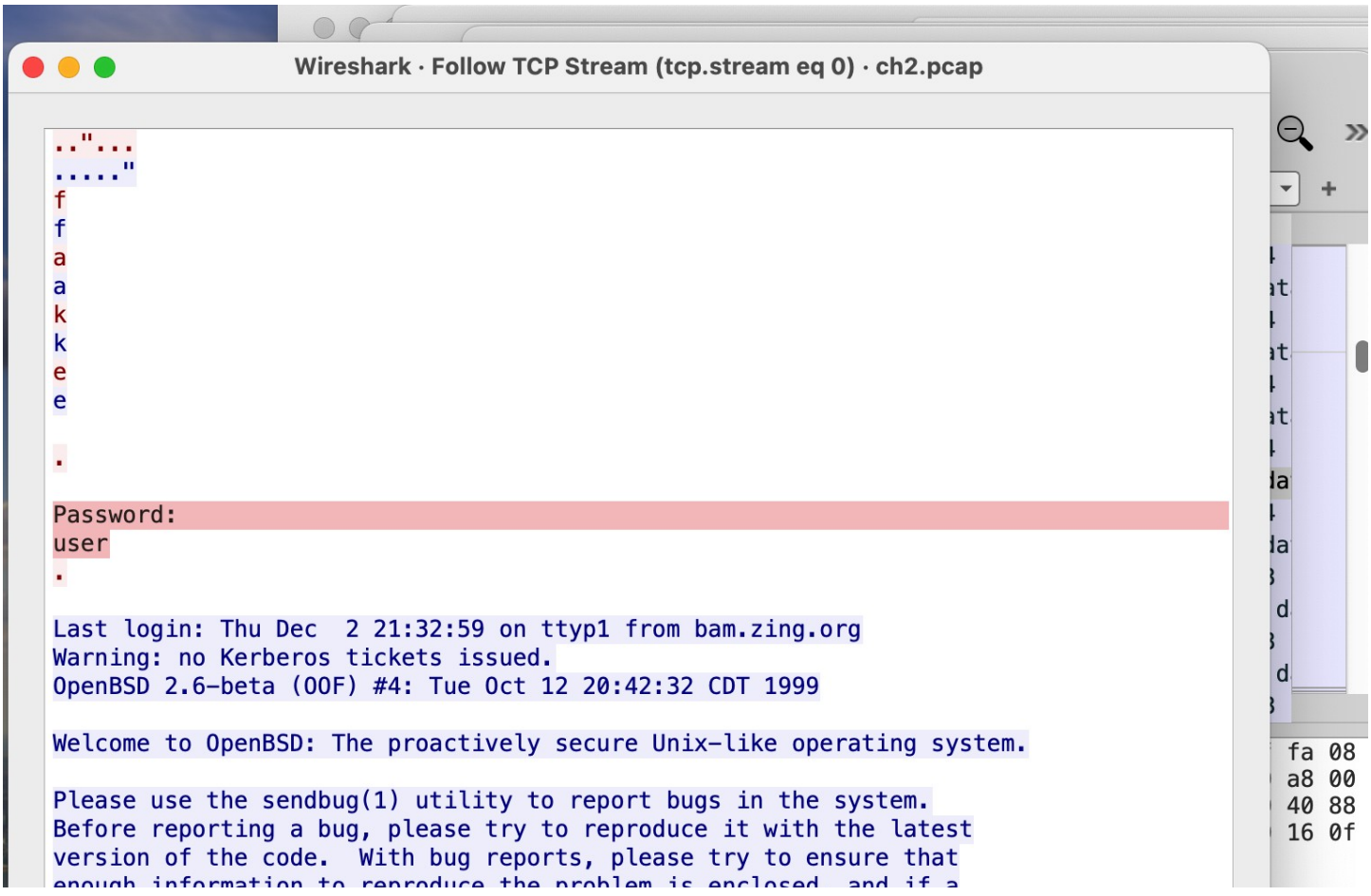


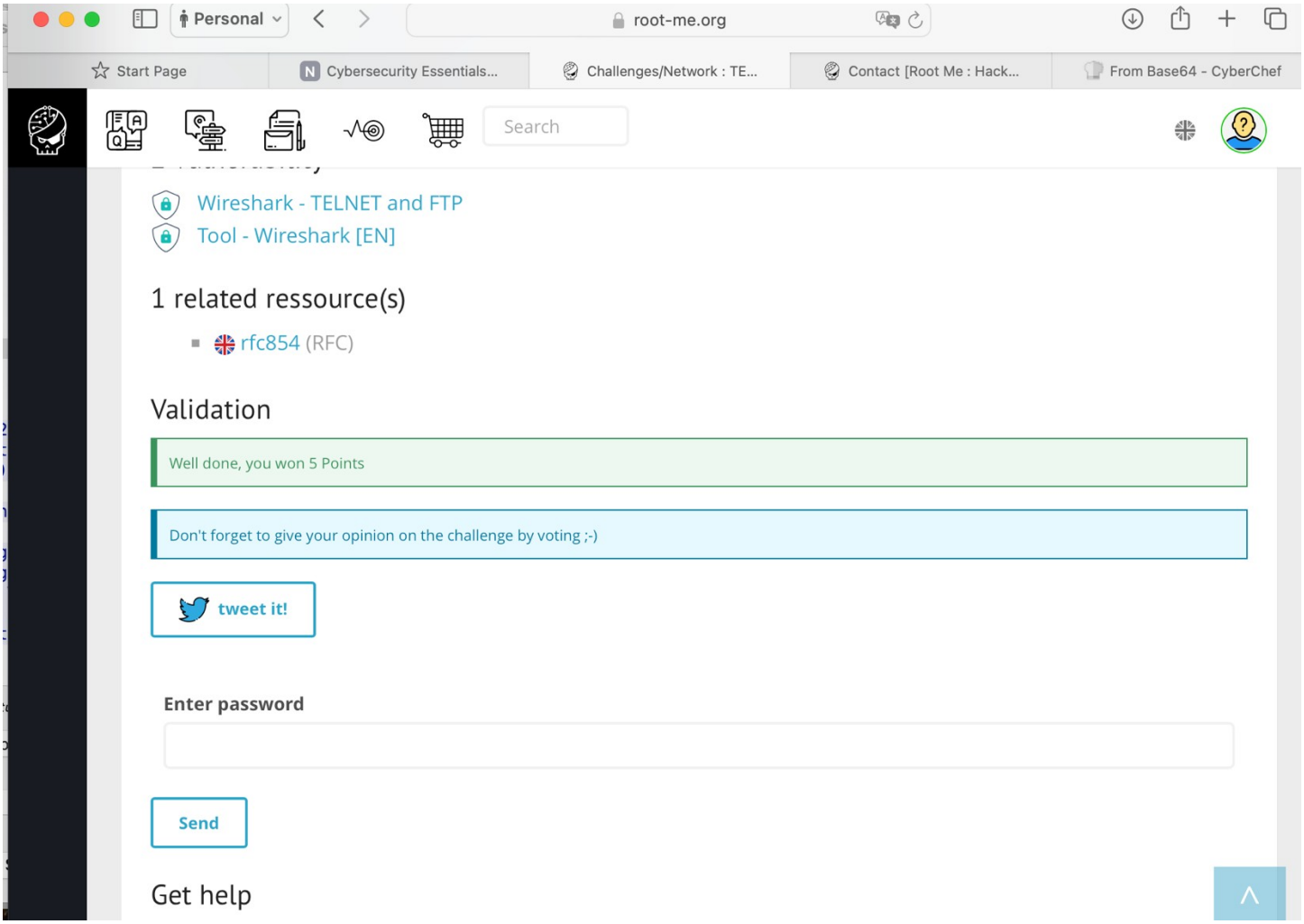




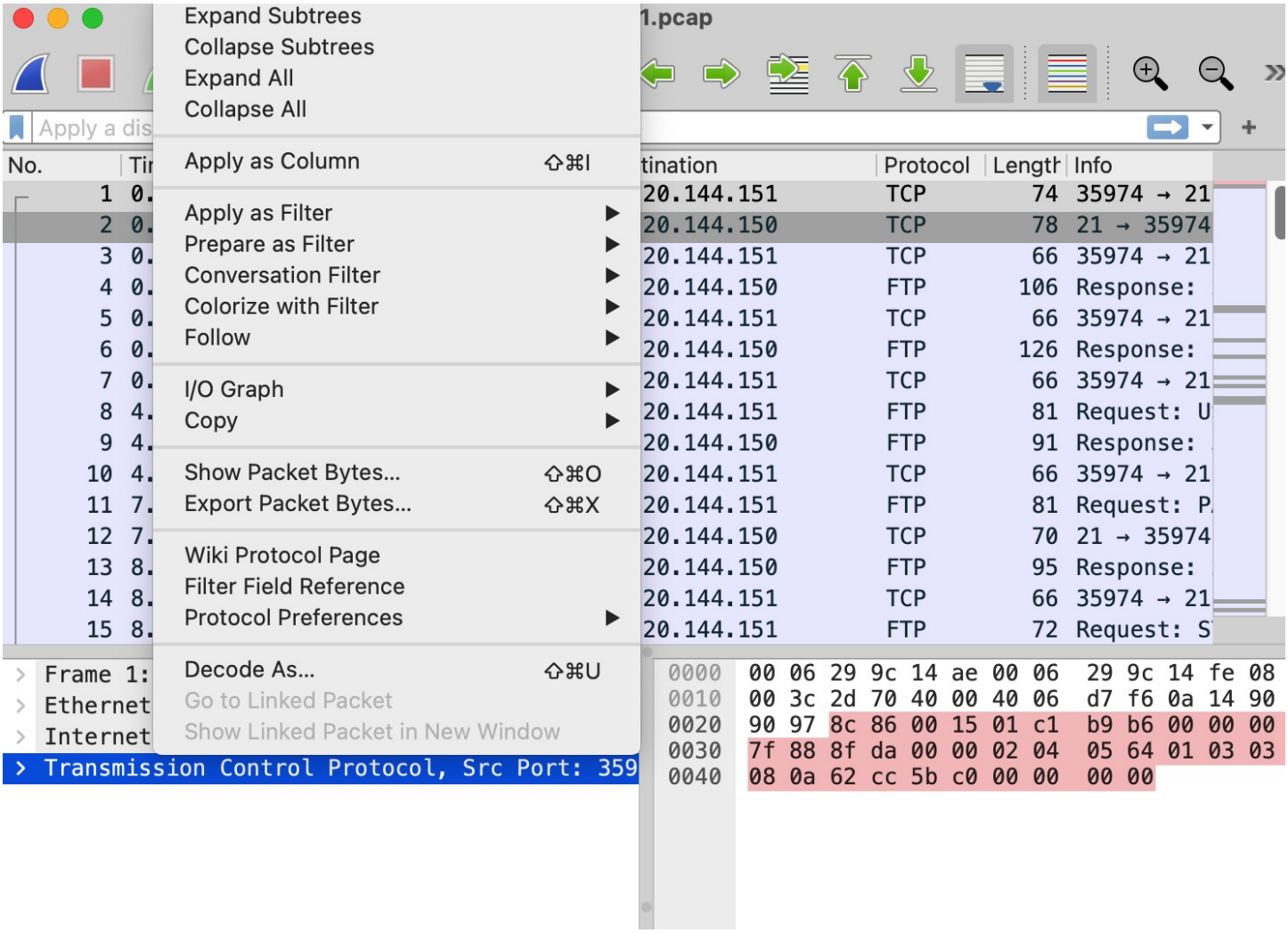
2. Root me: Telnet - authentication

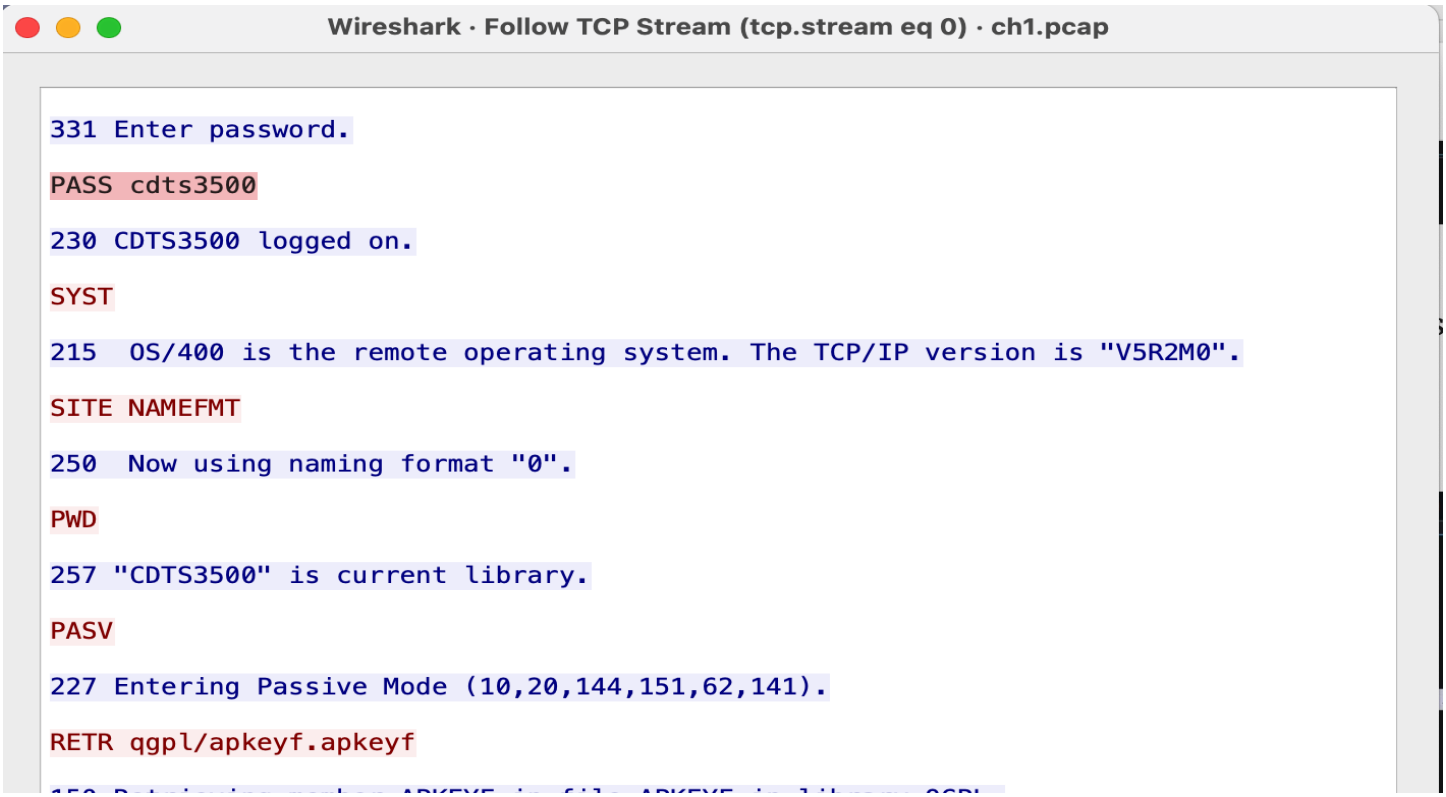

ch2.pcap
tcp.stream eq 0
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.0.2 192.168.0.1 TCP 74 1254 → 23
2 TCP 74 23 → 1254
3 TCP 66 1254 → 23
4 TELNET 93 Do Suppres
5 TELNET 69 Do Authent
6 TCP 66 1254 → 23
7 TELNET 69 Won't Auth
8 TCP 66 23 → 1254
9 TELNET 91 Will Suppr
10 TELNET 130 Suboption
11 TCP 66 23 → 1254
12 TELNET 84 Do New Env
13 TELNET 75 Don't Encr
14 TCP 66 23 → 1254
15 TELNET 90 Suboption
Mark/Unmark Selected ⌘M
Ignore/Unignore Selected ⌘D
Set/Unset Time Reference ⌘T
Time Shift... ⇧⌘T
Packet Comments
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
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

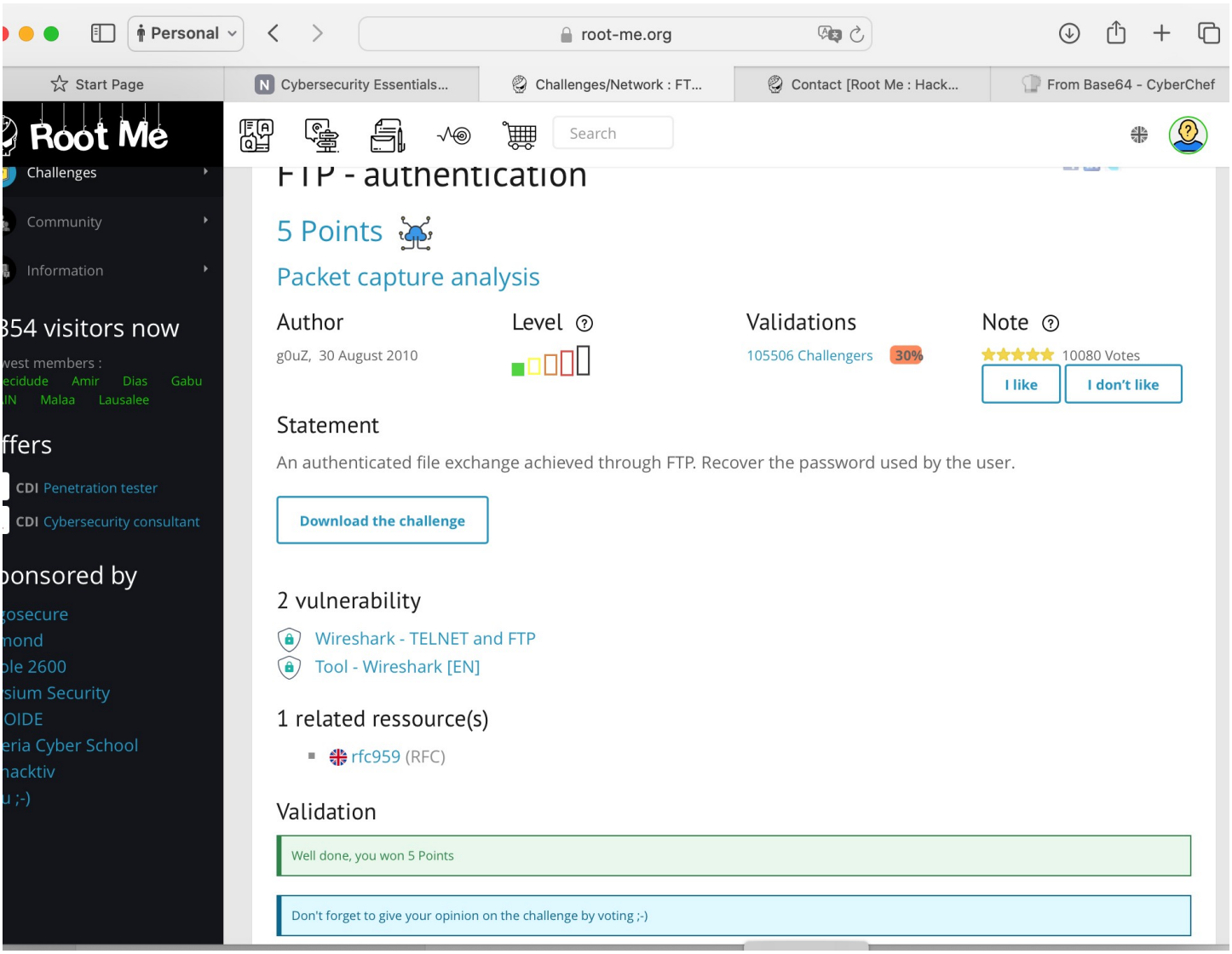

Wireshark · Follow TCP Stream (tcp.stream eq 0) · ch2.pcap
..".....
.....".
f
f
a
a
k
k
e
e
.
Password:
user
.
Last login: Thu Dec 2 21:32:59 on ttyp1 from bam.zing.org
Warning: no Kerberos tickets issued.
OpenBSD 2.6-beta (OOF) #4: Tue Oct 12 20:42:32 CDT 1999
Welcome to OpenBSD: The proactively secure 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
fa 08
a8 00
40 88
16 0f



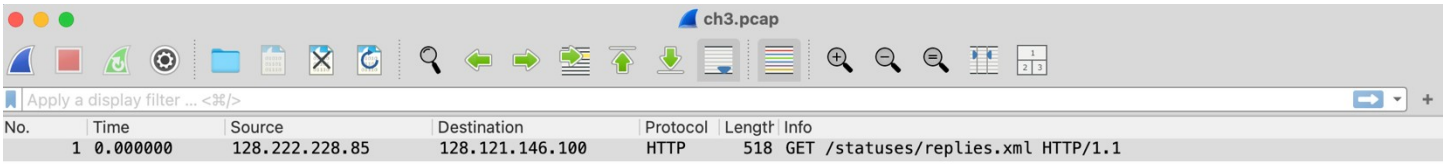
3. **Root me: Ftp - authentication**

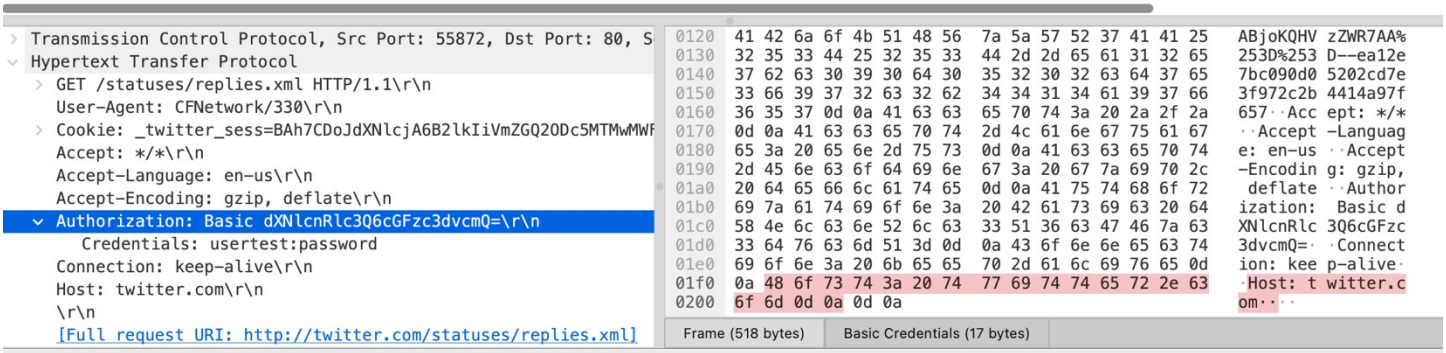

Expand Subtrees
Collapse Subtrees
Expand All
Collapse All
Apply as Column ⇧⌘I
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize with Filter
Follow
I/O Graph
Copy
Show Packet Bytes... ⇧⌘O
Export Packet Bytes... ⇧⌘X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As... ⇧⌘U
Go to Linked Packet
Show Linked Packet in New Window
1.pcap
No.
tination
Protocol
Length
Info
20.144.151 TCP 74 35974 → 21
20.144.150 TCP 78 21 → 35974
20.144.151 TCP 66 35974 → 21
20.144.150 FTP 106 Response:
20.144.151 TCP 66 35974 → 21
20.144.150 FTP 126 Response:
20.144.151 TCP 66 35974 → 21
20.144.151 FTP 81 Request: U
20.144.150 FTP 91 Response:
20.144.151 TCP 66 35974 → 21
20.144.151 FTP 81 Request: P
20.144.150 TCP 70 21 → 35974
20.144.150 FTP 95 Response:
20.144.151 TCP 66 35974 → 21
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

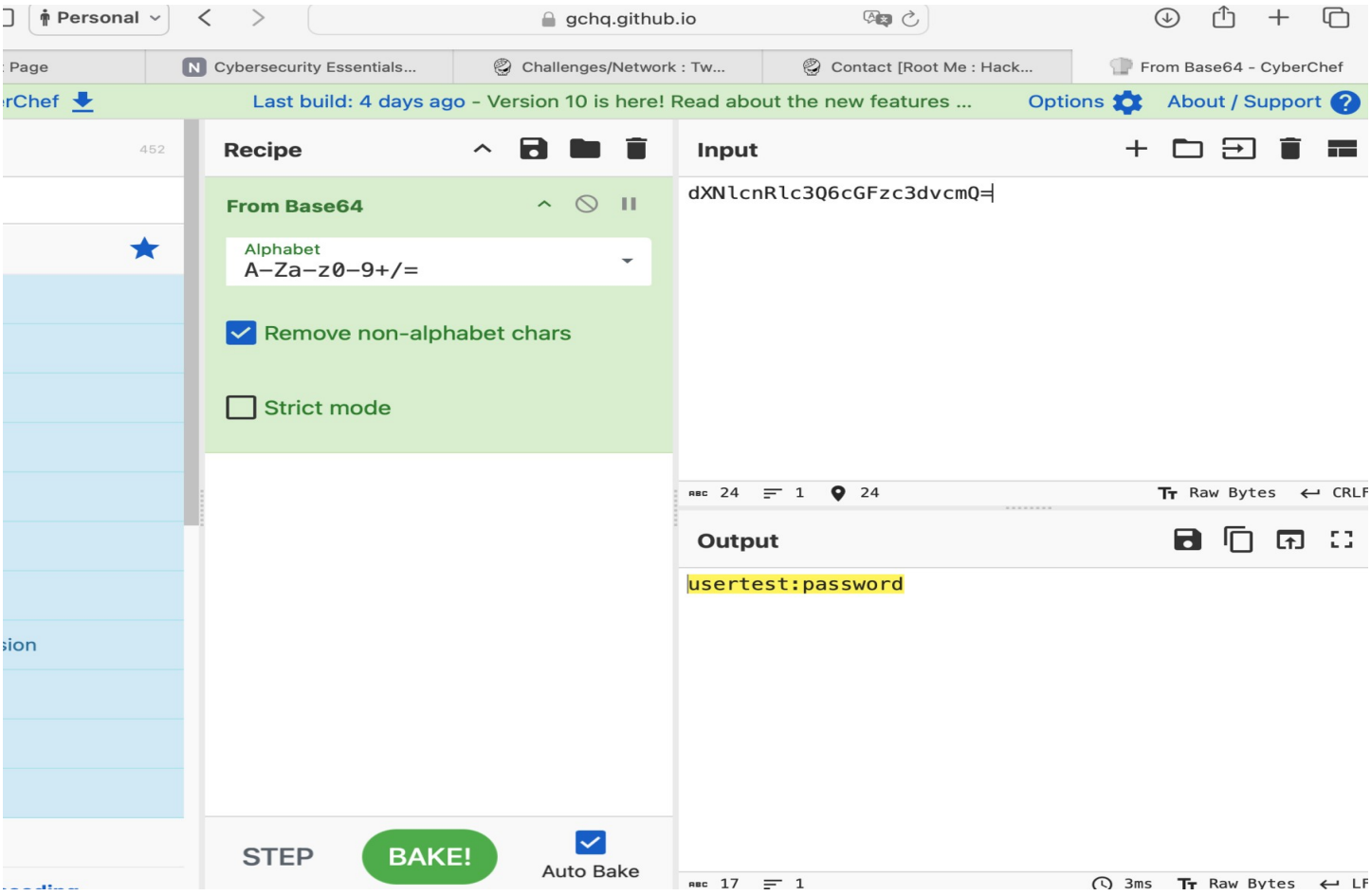

Wireshark · Follow TCP Stream (tcp.stream eq 0) · ch1.pcap
331 Enter password.
PASS cdts3500
230 CDTS3500 logged on.
SYST
215 OS/400 is the remote operating system. The TCP/IP version is "V5R2M0".
SITE NAMEFMT
250 Now using naming format "0".
PWD
257 "CDTS3500" is current library.
PASV
227 Entering Passive Mode (10,20,144,151,62,141).
RETR qgpl/apkeyf.apkeyf

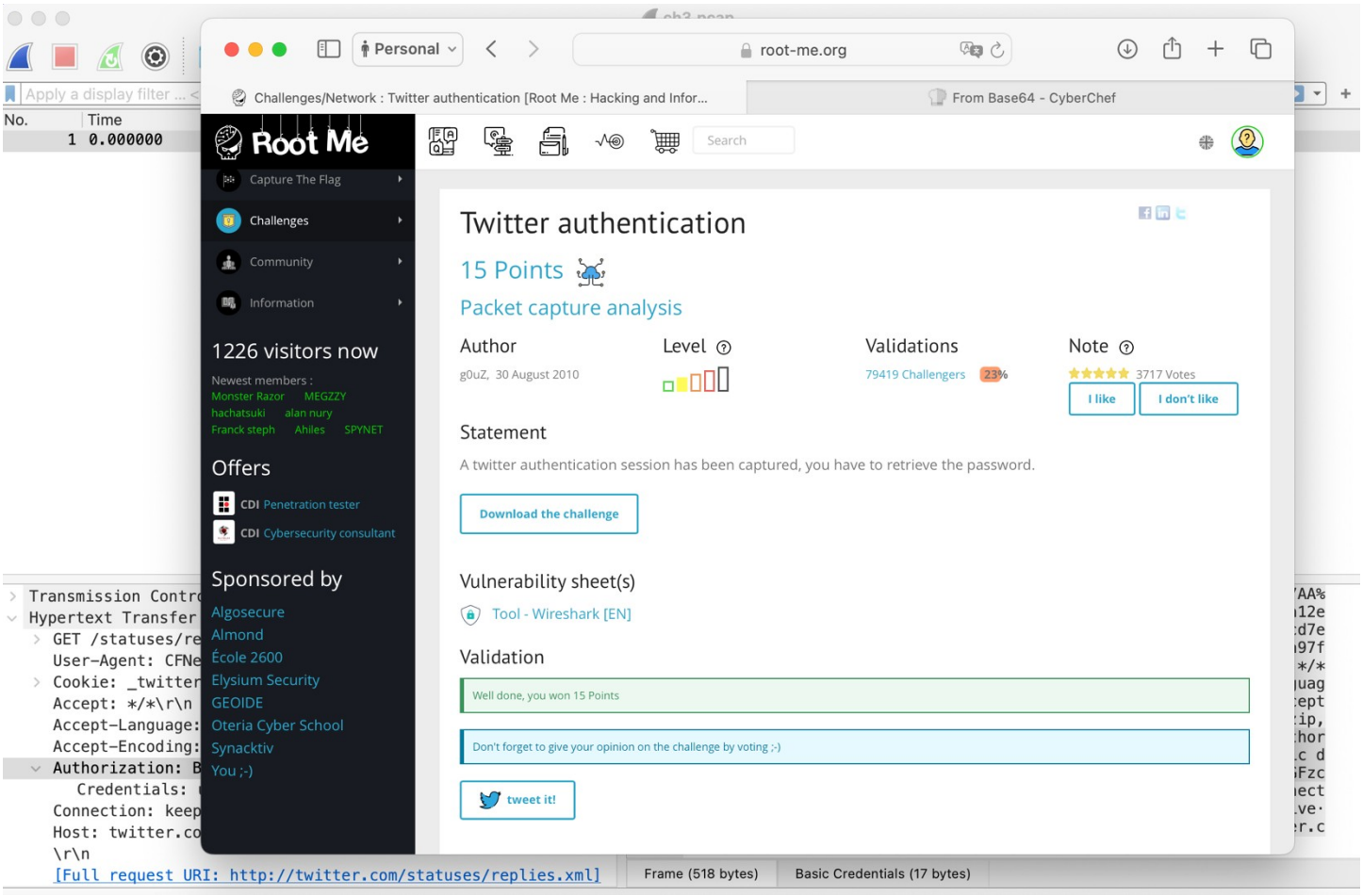


4. Root me: Twitter authentication

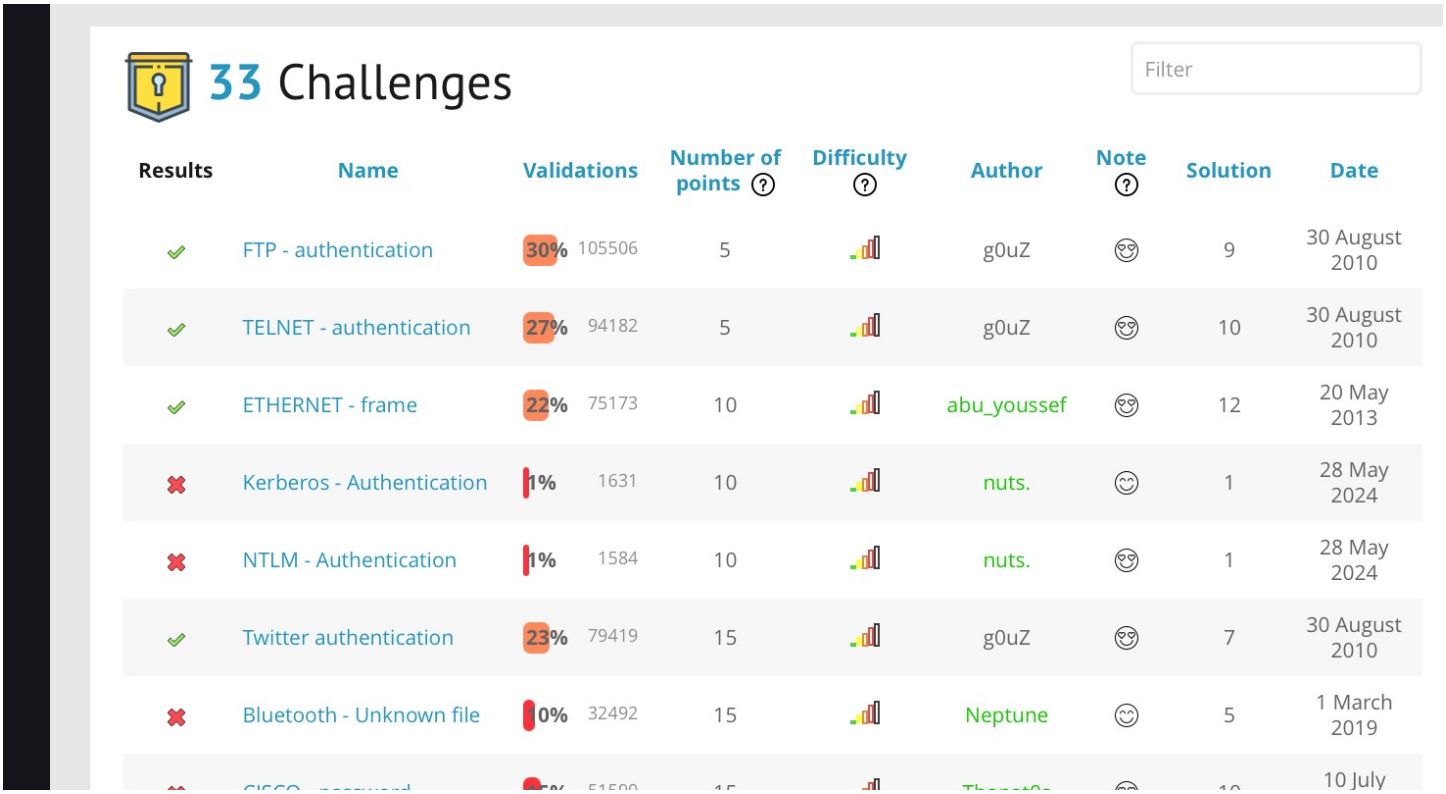

ch3.pcap
Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length Info
1 0.000000 128.222.228.85 128.121.146.100 HTTP 518 GET /statuses/replies.xml HTTP/1.1


Transmission Control Protocol, Src Port: 55872, Dst Port: 80, S
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
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··
Frame (518 bytes)
Basic Credentials (17 bytes)

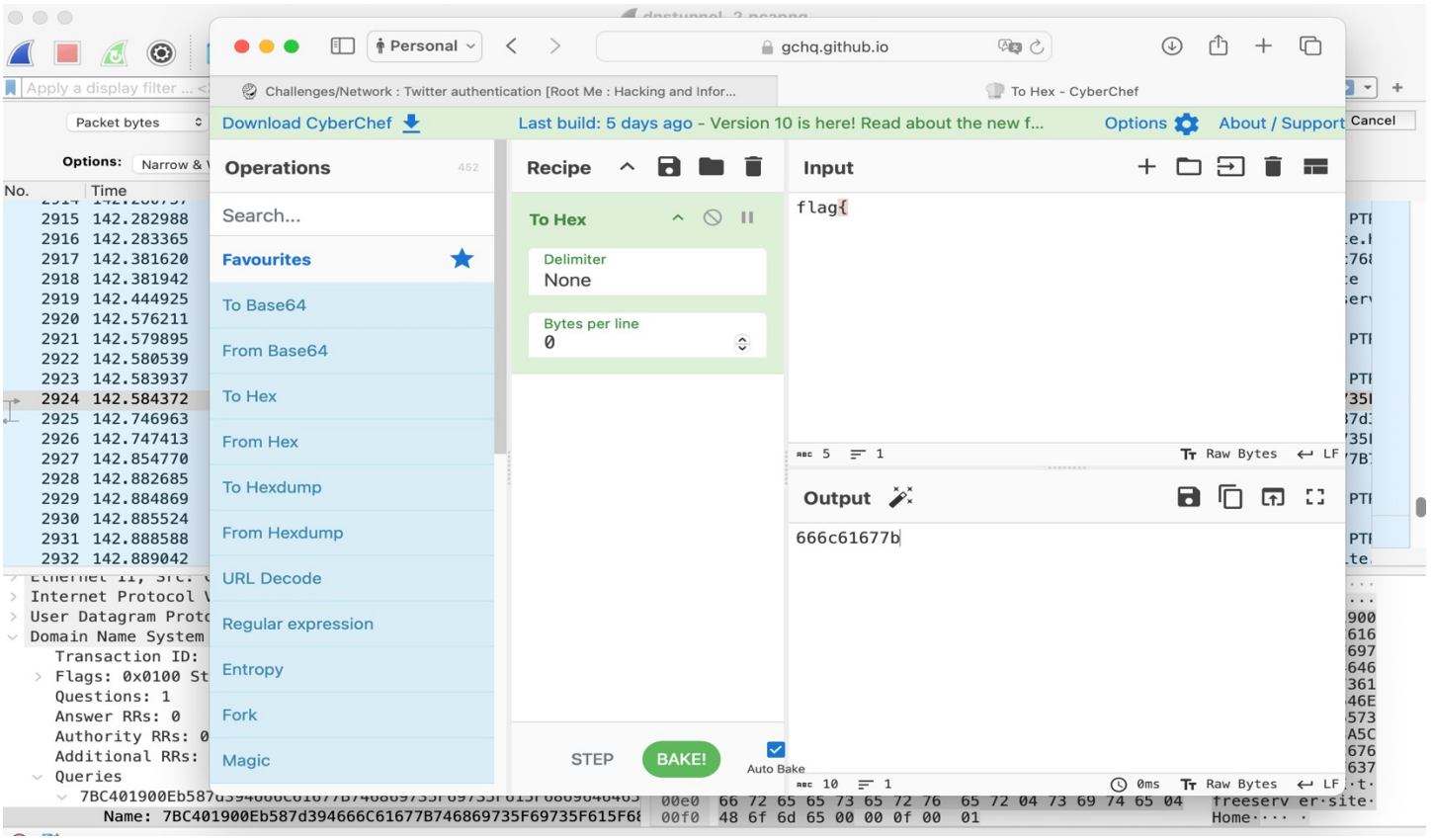

gchq.github.io
Page
Cybersecurity Essentials...
Challenges/Network : Tw...
Contact [Root Me : Hack...
From Base64 - CyberChef
Last build: 4 days ago - Version 10 is here! Read about the new features ...
Options
About / Support
Recipe
From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars
Strict mode
STEP
BAKE!
Auto Bake
Input
dXNlcnRlc3Q6cGFzc3dvcmQ=
24 1 24 Raw Bytes CRLF
Output
usertest:password
17 1 3ms Raw Bytes LF

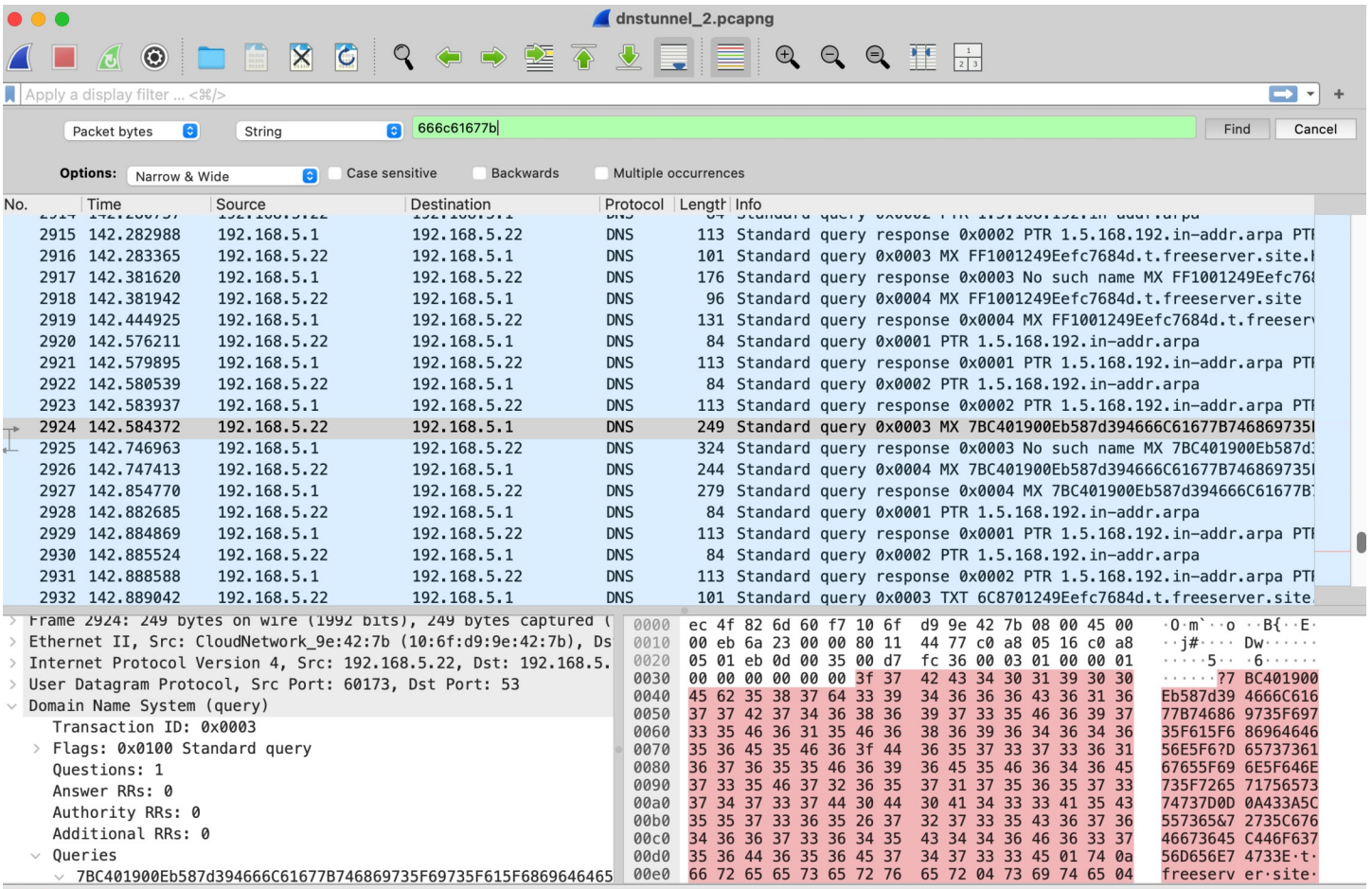


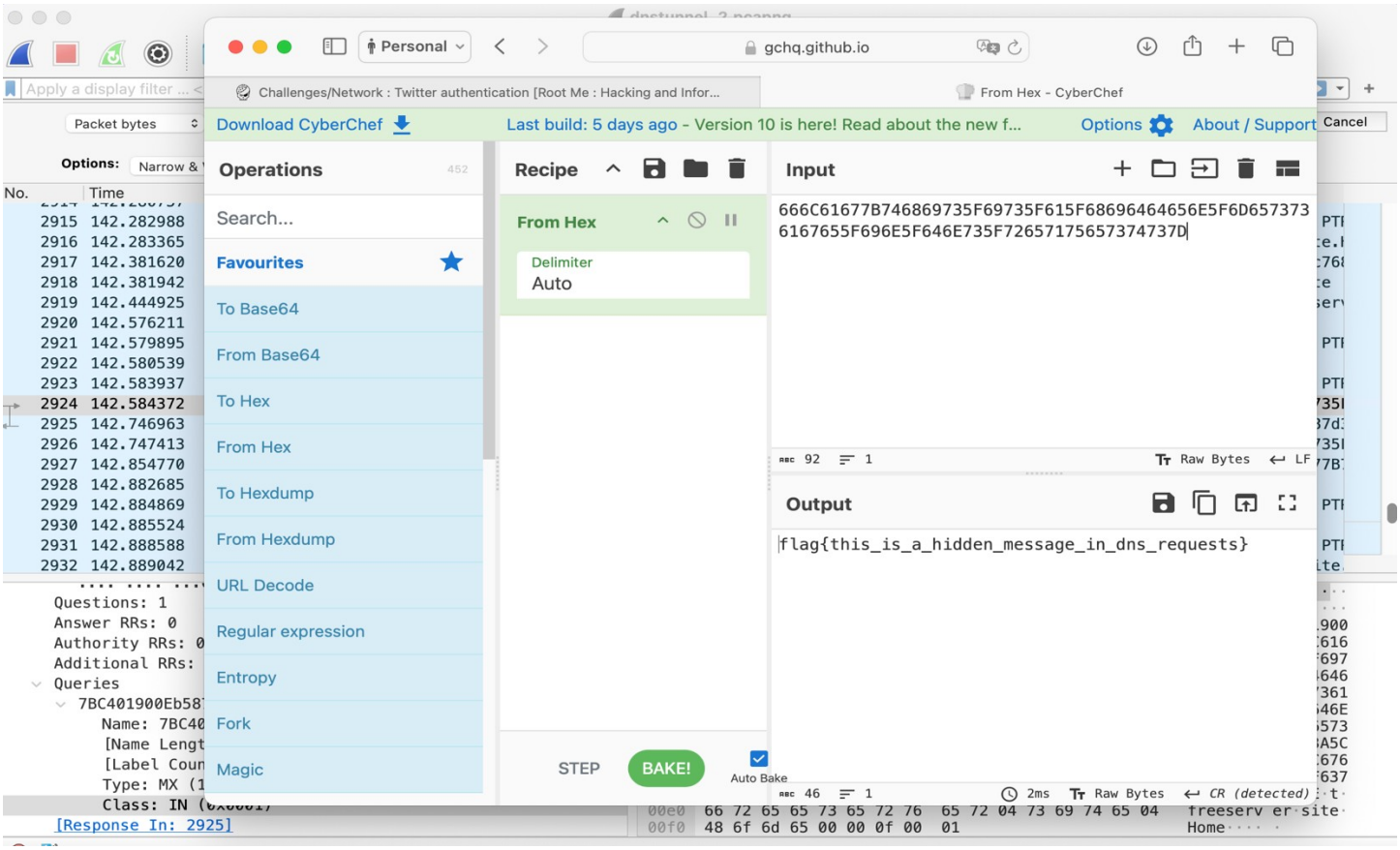
All completed root me challenges:



5. **DNS tunnel**


gchq.github.io
Challenges/Network : Twitter authentication [Root Me : Hacking and Infor...
To Hex - CyberChef
Download CyberChef
Last build: 5 days ago - Version 10 is here! Read about the new f...
Options
About / Support
Operations
Search...
Favourites
To Base64
From Base64
To Hex
From Hex
To Hexdump
From Hexdump
URL Decode
Regular expression
Entropy
Fork
Magic
Recipe
To Hex
Delimiter
None
Bytes per line
0
Input
flag{
Raw Bytes
Output
666c61677b
STEP
BAKE!
Auto Bake


dnstunnel_2.pcapng
Packet bytes
String
666c61677b
Find
Cancel
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
2916 142.283365 192.168.5.22 192.168.5.1 DNS 101 Standard query 0x0003 MX FF1001249Eefc7684d.t.freeserver.site
2917 142.381620 192.168.5.1 192.168.5.22 DNS 176 Standard query response 0x0003 No such name MX FF1001249Eefc7684d.t.freeserver.site
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.freeserver.site
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
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
2924 142.584372 192.168.5.22 192.168.5.1 DNS 249 Standard query 0x0003 MX 7BC401900Eb587d394666C61677B746869735F69735F615F6869646465.t.freeserver.site
2925 142.746963 192.168.5.1 192.168.5.22 DNS 324 Standard query response 0x0003 No such name MX 7BC401900Eb587d394666C61677B746869735F69735F615F6869646465.t.freeserver.site
2926 142.747413 192.168.5.22 192.168.5.1 DNS 244 Standard query 0x0004 MX 7BC401900Eb587d394666C61677B746869735F69735F615F6869646465.t.freeserver.site
2927 142.854770 192.168.5.1 192.168.5.22 DNS 279 Standard query response 0x0004 MX 7BC401900Eb587d394666C61677B746869735F69735F615F6869646465.t.freeserver.site
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
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
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
Domain Name System (query)
Transaction ID: 0x0003
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
7BC401900Eb587d394666C61677B746869735F69735F615F6869646465
0000 ec 4f 82 6d 60 f7 10 6f d9 9e 42 7b 08 00 45 00
0010 00 eb 6a 23 00 00 80 11 44 77 c0 a8 05 16 c0 a8
0020 05 01 eb 0d 00 35 00 d7 fc 36 00 03 01 00 00 01
0030 00 00 00 00 00 00 3f 37 42 43 34 30 31 39 30 30
0040 45 62 35 38 37 64 33 39 34 36 36 36 43 36 31 36
0050 37 37 42 37 34 36 38 36 39 37 33 35 46 36 39 37
0060 33 35 46 36 31 35 46 36 38 36 39 36 34 36 34 36
0070 35 36 45 35 46 36 3f 44 36 35 37 33 37 33 36 31
0080 36 37 36 35 35 46 36 39 36 45 35 46 36 34 36 45
0090 37 33 35 46 37 32 36 35 37 31 37 35 36 35 37 33
00a0 37 34 37 33 37 44 30 44 30 41 34 33 33 41 35 43
00b0 35 35 37 33 36 35 26 37 32 37 33 35 43 36 37 36
00c0 34 36 36 37 33 36 34 35 43 34 34 36 46 36 33 37
00d0 35 36 44 36 35 36 45 37 34 37 33 33 45 01 74 0a
00e0 66 72 65 65 73 65 72 76 65 72 04 73 69 74 65 04
freeserv er·site·


gchq.github.io
Challenges/Network : Twitter authentication [Root Me : Hacking and Infor...
From Hex - CyberChef
Download CyberChef
Last build: 5 days ago - Version 10 is here! Read about the new f...
Options
About / Support
Operations
Search...
Favourites
To Base64
From Base64
To Hex
From Hex
To Hexdump
From Hexdump
URL Decode
Regular expression
Entropy
Fork
Magic
Recipe
From Hex
Delimiter
Auto
Input
666C61677B746869735F69735F615F68696464656E5F6D6573736167655F696E5F646E735F72657175657374737D
Raw Bytes
LF
Output
flag{this_is_a_hidden_message_in_dns_requests}
STEP
BAKE!
Auto Bake
Raw Bytes
CR (detected)