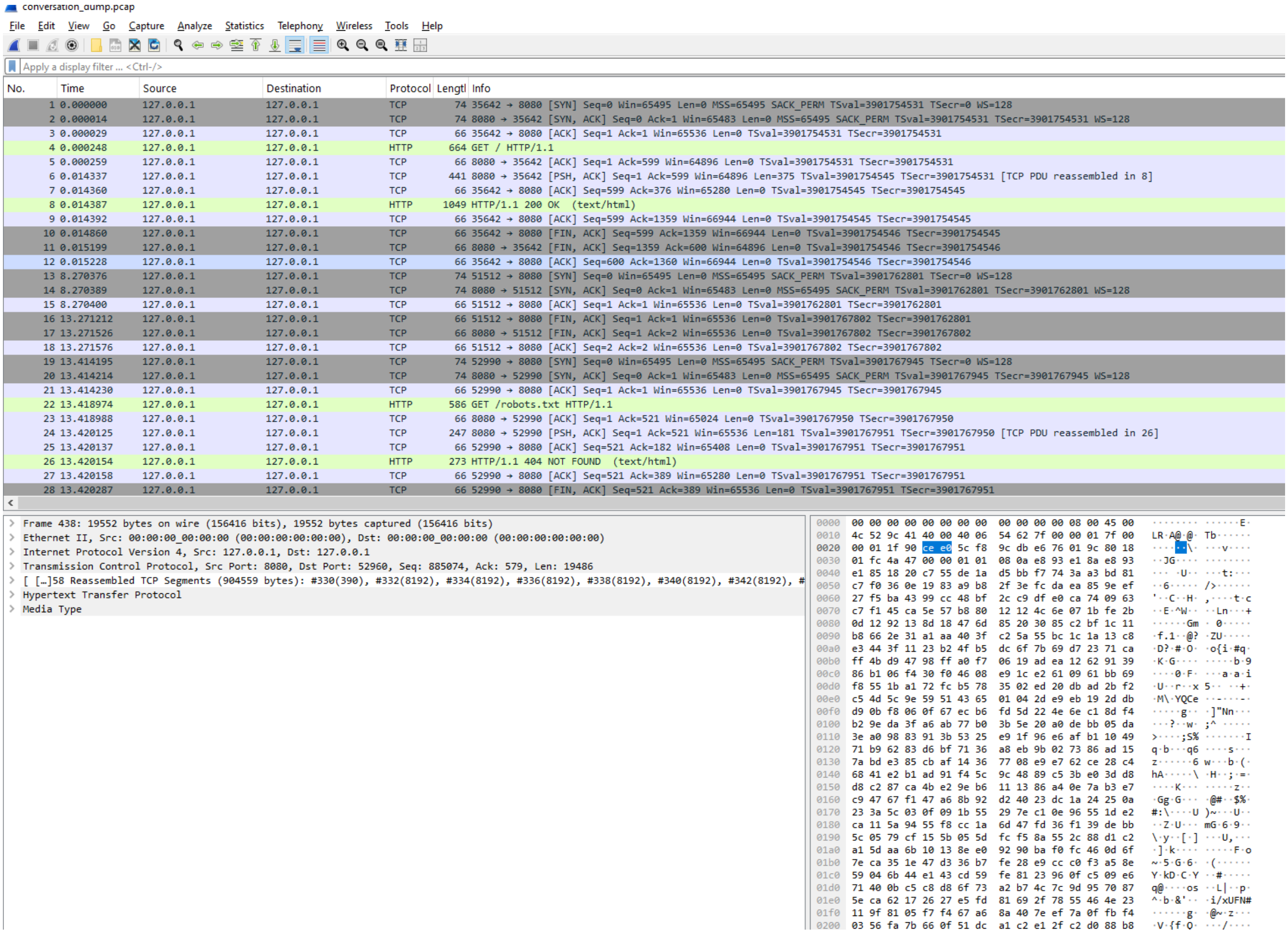
In this challenge we are given a .pcap file

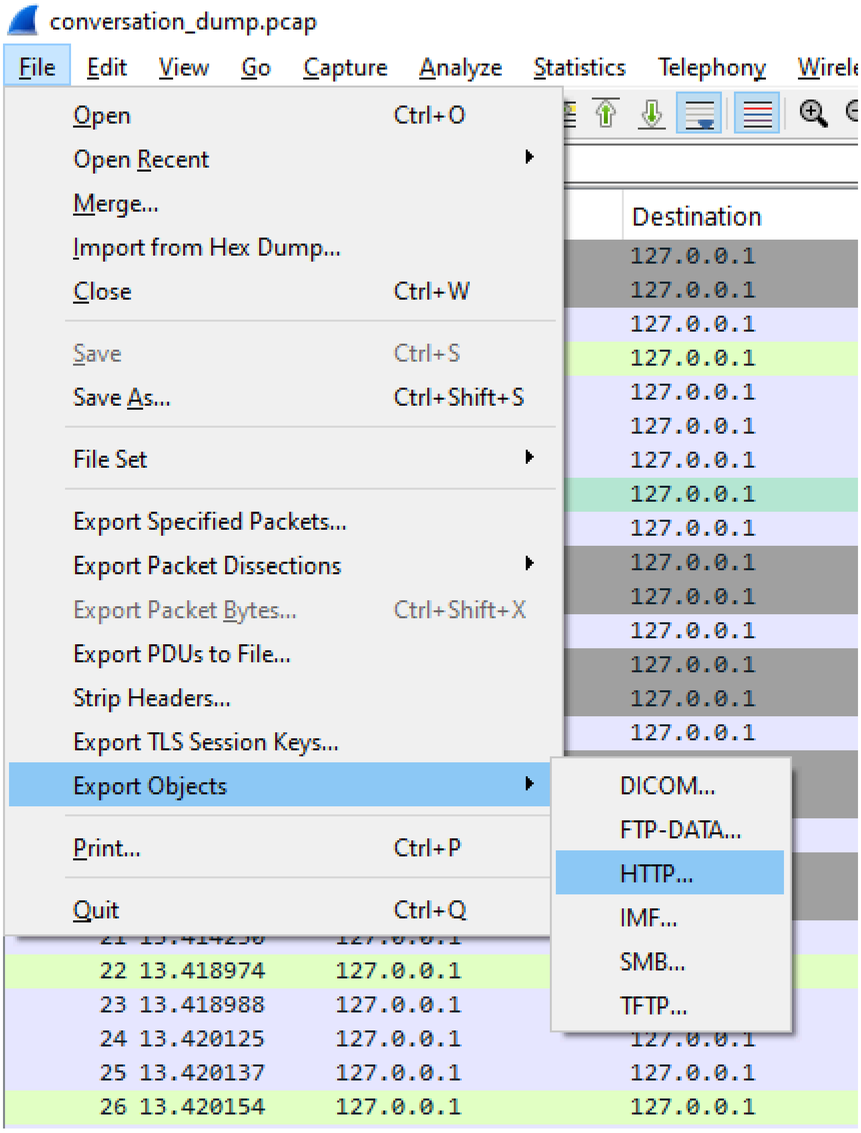

conversation_dump.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time      Source     Destination  Protocol Lengtl Info
   1 0.000000  127.0.0.1  127.0.0.1    TCP        74 35642 → 8080 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM TSval=3901754531 TSecr=0 WS=128
   2 0.000014  127.0.0.1  127.0.0.1    TCP        74 8080 → 35642 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM TSval=3901754531 TSecr=3901754531 WS=128
   3 0.000029  127.0.0.1  127.0.0.1    TCP        66 35642 → 8080 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=3901754531 TSecr=3901754531
   4 0.000248  127.0.0.1  127.0.0.1    HTTP      664 GET / HTTP/1.1
   5 0.000259  127.0.0.1  127.0.0.1    TCP        66 8080 → 35642 [ACK] Seq=1 Ack=599 Win=64896 Len=0 TSval=3901754531 TSecr=3901754531
   6 0.014337  127.0.0.1  127.0.0.1    TCP       441 8080 → 35642 [PSH, ACK] Seq=1 Ack=599 Win=64896 Len=375 TSval=3901754545 TSecr=3901754531 [TCP PDU reassembled in 8]
   7 0.014360  127.0.0.1  127.0.0.1    TCP        66 35642 → 8080 [ACK] Seq=599 Ack=376 Win=65280 Len=0 TSval=3901754545 TSecr=3901754545
   8 0.014387  127.0.0.1  127.0.0.1    HTTP     1049 HTTP/1.1 200 OK  (text/html)
   9 0.014392  127.0.0.1  127.0.0.1    TCP        66 35642 → 8080 [ACK] Seq=599 Ack=1359 Win=66944 Len=0 TSval=3901754545 TSecr=3901754545
  10 0.014860  127.0.0.1  127.0.0.1    TCP        66 35642 → 8080 [FIN, ACK] Seq=599 Ack=1359 Win=66944 Len=0 TSval=3901754546 TSecr=3901754545
  11 0.015199  127.0.0.1  127.0.0.1    TCP        66 8080 → 35642 [FIN, ACK] Seq=1359 Ack=600 Win=64896 Len=0 TSval=3901754546 TSecr=3901754546
  12 0.015228  127.0.0.1  127.0.0.1    TCP        66 35642 → 8080 [ACK] Seq=600 Ack=1360 Win=66944 Len=0 TSval=3901754546 TSecr=3901754546
  13 8.270376  127.0.0.1  127.0.0.1    TCP        74 51512 → 8080 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM TSval=3901762801 TSecr=0 WS=128
  14 8.270389  127.0.0.1  127.0.0.1    TCP        74 8080 → 51512 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM TSval=3901762801 TSecr=3901762801 WS=128
  15 8.270400  127.0.0.1  127.0.0.1    TCP        66 51512 → 8080 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=3901762801 TSecr=3901762801
  16 13.271212 127.0.0.1  127.0.0.1    TCP        66 51512 → 8080 [FIN, ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=3901767802 TSecr=3901762801
  17 13.271526 127.0.0.1  127.0.0.1    TCP        66 8080 → 51512 [FIN, ACK] Seq=1 Ack=2 Win=65536 Len=0 TSval=3901767802 TSecr=3901767802
  18 13.271576 127.0.0.1  127.0.0.1    TCP        66 51512 → 8080 [ACK] Seq=2 Ack=2 Win=65536 Len=0 TSval=3901767802 TSecr=3901767802
  19 13.414195 127.0.0.1  127.0.0.1    TCP        74 52990 → 8080 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM TSval=3901767945 TSecr=0 WS=128
  20 13.414214 127.0.0.1  127.0.0.1    TCP        74 8080 → 52990 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM TSval=3901767945 TSecr=3901767945 WS=128
  21 13.414230 127.0.0.1  127.0.0.1    TCP        66 52990 → 8080 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=3901767945 TSecr=3901767945
  22 13.418974 127.0.0.1  127.0.0.1    HTTP      586 GET /robots.txt HTTP/1.1
  23 13.418988 127.0.0.1  127.0.0.1    TCP        66 8080 → 52990 [ACK] Seq=1 Ack=521 Win=65024 Len=0 TSval=3901767950 TSecr=3901767950
  24 13.420125 127.0.0.1  127.0.0.1    TCP       247 8080 → 52990 [PSH, ACK] Seq=1 Ack=521 Win=65536 Len=181 TSval=3901767951 TSecr=3901767950 [TCP PDU reassembled in 26]
  25 13.420137 127.0.0.1  127.0.0.1    TCP        66 52990 → 8080 [ACK] Seq=521 Ack=182 Win=65408 Len=0 TSval=3901767951 TSecr=3901767951
  26 13.420154 127.0.0.1  127.0.0.1    HTTP      273 HTTP/1.1 404 NOT FOUND  (text/html)
  27 13.420158 127.0.0.1  127.0.0.1    TCP        66 52990 → 8080 [ACK] Seq=521 Ack=389 Win=65280 Len=0 TSval=3901767951 TSecr=3901767951
  28 13.420287 127.0.0.1  127.0.0.1    TCP        66 52990 → 8080 [FIN, ACK] Seq=521 Ack=389 Win=65536 Len=0 TSval=3901767951 TSecr=3901767951
```

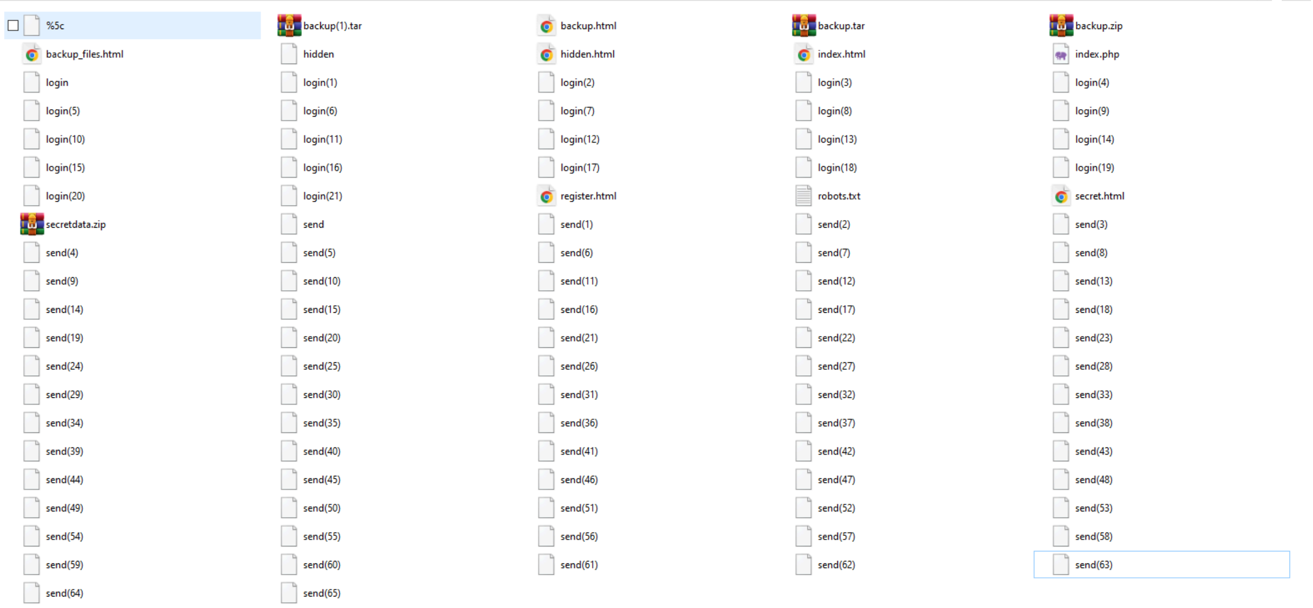
```
> Frame 438: 19552 bytes on wire (156416 bits), 19552 bytes captured (156416 bits)
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 8080, Dst Port: 52960, Seq: 885074, Ack: 579, Len: 19486
> [ […]58 Reassembled TCP Segments (904559 bytes): #330(390), #332(8192), #334(8192), #336(8192), #338(8192), #340(8192), #342(8192), #
> Hypertext Transfer Protocol
> Media Type
```

```
0000  00 00 00 00 00 00 00 00  00 00 00 00 08 00 45 00   ········ ······E·
0010  4c 52 9c 41 40 00 40 06  54 62 7f 00 00 01 7f 00   LR·A@·@· Tb······
0020  00 01 1f 90 ce e0 5c f8  9c db e6 76 01 9c 80 18   ······\· ···v····
0030  01 fc 4a 47 00 00 01 01  08 0a e8 93 e1 8a e8 93   ··JG···· ········
0040  e1 85 18 20 c7 55 de 1a  d5 bb f7 74 3a a3 bd 81   ··· ·U·· ···t:···
0050  c7 f0 36 0e 19 83 a9 b8  2f 3e fc da ea 85 9e ef   ··6····· />······
0060  27 f5 ba 43 99 cc 48 bf  2c c9 df e0 ca 74 09 63   '··C··H· ,····t·c
0070  c7 f1 45 ca 5e 57 b8 80  12 12 4c 6e 07 1b fe 2b   ··E·^W·· ··Ln···+
0080  0d 12 92 13 8d 18 47 6d  85 20 30 85 c2 bf 1c 11   ······Gm · 0·····
0090  b8 66 2e 31 a1 aa 40 3f  c2 5a 55 bc 1c 1a 13 c8   ·f.1··@? ·ZU·····
00a0  e3 44 3f 11 23 b2 4f b5  dc 6f 7b 69 d7 23 71 ca   ·D?·#·O· ·o{i·#q·
00b0  ff 4b d9 47 98 ff a0 f7  06 19 ad ea 12 62 91 39   ·K·G···· ·····b·9
00c0  86 b1 06 f4 30 f0 46 08  e9 1c e2 61 09 61 bb 69   ····0·F· ···a·a·i
00d0  f8 55 1b a1 72 fc b5 78  35 02 ed 20 db ad 2b f2   ·U··r··x 5·· ··+·
00e0  c5 4d 5c 9e 59 51 43 65  01 04 2d e9 eb 19 2d db   ·M\·YQCe ··-···-·
00f0  d9 0b f8 06 0f 67 ec b6  fd 5d 22 4e 6e c1 8d f4   ·····g·· ·]"Nn···
0100  b2 9e da 3f a6 ab 77 b0  3b 5e 20 a0 de bb 05 da   ···?··w· ;^ ·····
0110  3e a0 98 83 91 3b 53 25  e9 1f 96 e6 af b1 10 49   >····;S% ·······I
0120  71 b9 62 83 d6 bf 71 36  a8 eb 9b 02 73 86 ad 15   q·b···q6 ····s···
0130  7a bd e3 85 cb af 14 36  77 08 e9 e7 62 ce 28 c4   z······6 w···b·(·
0140  68 41 e2 b1 ad 91 f4 5c  9c 48 89 c5 3b e0 3d d8   hA·····\ ·H··;·=·
0150  d8 c2 87 ca 4b e2 9e b6  11 13 86 a4 0e 7a b3 e7   ····K··· ·····z··
0160  c9 47 67 f1 47 a6 8b 92  d2 40 23 dc 1a 24 25 0a   ·Gg·G··· ·@#··$%·
0170  23 3a 5c 03 0f 09 1b 55  29 7e c1 0e 96 55 1d e2   #:\····U )~···U··
0180  ca 11 5a 94 55 f8 cc 1a  6d 47 fd 36 f1 39 de bb   ··Z·U··· mG·6·9··
0190  5c 05 79 cf 15 5b 05 5d  fc f5 8a 55 2c 88 d1 c2   \·y··[·] ···U,···
01a0  a1 5d aa 6b 10 13 8e e0  92 90 ba f0 fc 46 0d 6f   ·]·k···· ·····F·o
01b0  7e ca 35 1e 47 d3 36 b7  fe 28 e9 cc c0 f3 a5 8e   ~·5·G·6· ·(······
01c0  59 04 6b 44 e1 43 cd 59  fe 81 23 96 0f c5 09 e6   Y·kD·C·Y ··#·····
01d0  71 40 0b c5 c8 d8 6f 73  a2 b7 4c 7c 9d 95 70 87   q@····os ··L|··p·
01e0  5e ca 62 17 26 27 e5 fd  81 69 2f 78 55 46 4e 23   ^·b·&'·· ·i/xUFN#
01f0  11 9f 81 05 f7 f4 67 a6  8a 40 7e ef 7a 0f fb f4   ······g· ·@~·z···
0200  03 56 fa 7b 66 0f 51 dc  a1 c2 e1 2f c2 d0 88 b8   ·V·{f·Q· ···/····
```

After we open it in Wireshark, and checking some HTTP packets, we see that we some some HTML files and others



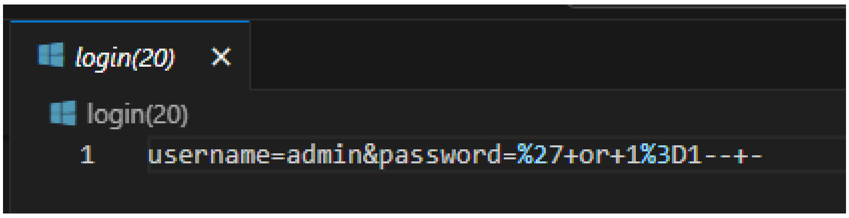
After this we export the HTTP objects to a now folder



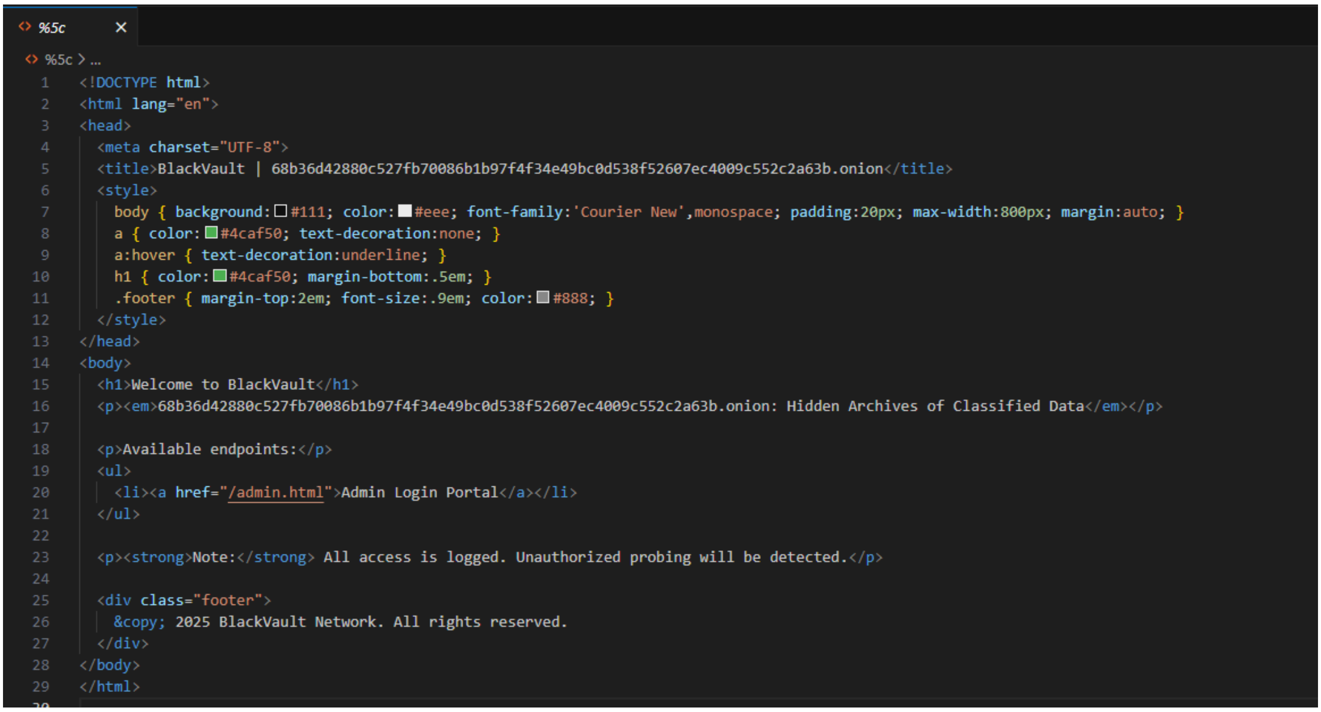
```
%5c              backup(1).tar    backup.html      backup.tar       backup.zip
backup_files.html hidden          hidden.html      index.html       index.php
login            login(1)         login(2)         login(3)         login(4)
login(5)         login(6)         login(7)         login(8)         login(9)
login(10)        login(11)        login(12)        login(13)        login(14)
login(15)        login(16)        login(17)        login(18)        login(19)
login(20)        login(21)        register.html    robots.txt       secret.html
secretdata.zip   send             send(1)          send(2)          send(3)
send(4)          send(5)          send(6)          send(7)          send(8)
send(9)          send(10)         send(11)         send(12)         send(13)
send(14)         send(15)         send(16)         send(17)         send(18)
send(19)         send(20)         send(21)         send(22)         send(23)
send(24)         send(25)         send(26)         send(27)         send(28)
send(29)         send(30)         send(31)         send(32)         send(33)
send(34)         send(35)         send(36)         send(37)         send(38)
send(39)         send(40)         send(41)         send(42)         send(43)
send(44)         send(45)         send(46)         send(47)         send(48)
send(49)         send(50)         send(51)         send(52)         send(53)
send(54)         send(55)         send(56)         send(57)         send(58)
send(59)         send(60)         send(61)         send(62)         send(63)
send(64)         send(65)
```

We have those files

The login, login(2), login (4) and so on (with even numbers) are a hacker's tries to log in with the last one being succesful after doing an injection



```
username=admin&password=%27+or+1%3D1--+-
```



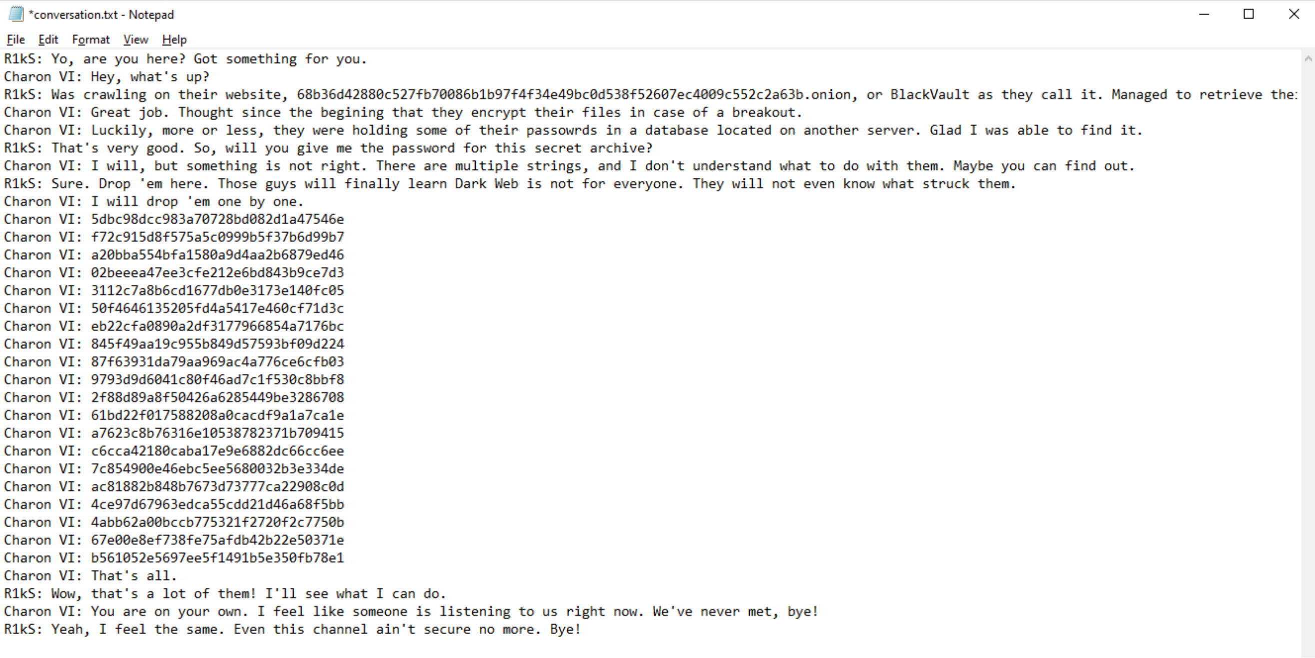
```html
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <title>BlackVault | 68b36d42880c527fb70086b1b97f4f34e49bc0d538f52607ec4009c552c2a63b.onion</title>
  <style>
    body { background:#111; color:#eee; font-family:'Courier New',monospace; padding:20px; max-width:800px; margin:auto; }
    a { color:#4caf50; text-decoration:none; }
    a:hover { text-decoration:underline; }
    h1 { color:#4caf50; margin-bottom:.5em; }
    .footer { margin-top:2em; font-size:.9em; color:#888; }
  </style>
</head>
<body>
  <h1>Welcome to BlackVault</h1>
  <p><em>68b36d42880c527fb70086b1b97f4f34e49bc0d538f52607ec4009c552c2a63b.onion: Hidden Archives of Classified Data</em></p>

  <p>Available endpoints:</p>
  <ul>
    <li><a href="/admin.html">Admin Login Portal</a></li>
  </ul>

  <p><strong>Note:</strong> All access is logged. Unauthorized probing will be detected.</p>

  <div class="footer">
    &copy; 2025 BlackVault Network. All rights reserved.
  </div>
</body>
</html>
```

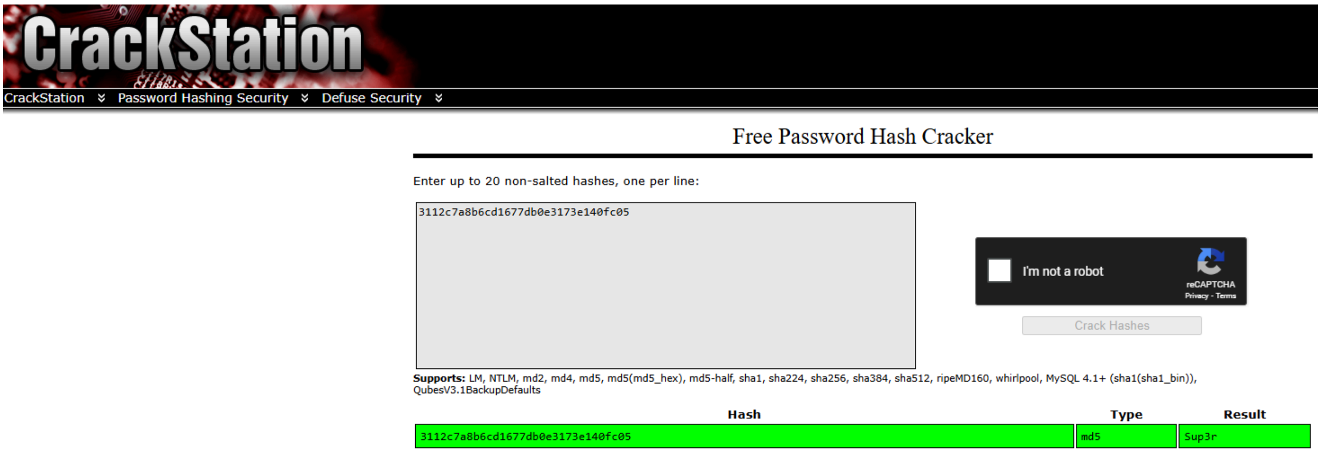
Afterwards, by inspecting the 66 'send' files, we can see a conversation between R1kS and Charon VI:



```
R1kS: Yo, are you here? Got something for you.
Charon VI: Hey, what's up?
R1kS: Was crawling on their website, 68b36d42880c527fb70086b1b97f4f34e49bc0d538f52607ec4009c552c2a63b.onion, or BlackVault as they call it. Managed to retrieve the:
Charon VI: Great job. Thought since the begining that they encrypt their files in case of a breakout.
Charon VI: Luckily, more or less, they were holding some of their passowrds in a database located on another server. Glad I was able to find it.
R1kS: That's very good. So, will you give me the password for this secret archive?
Charon VI: I will, but something is not right. There are multiple strings, and I don't understand what to do with them. Maybe you can find out.
R1kS: Sure. Drop 'em here. Those guys will finally learn Dark Web is not for everyone. They will not even know what struck them.
Charon VI: I will drop 'em one by one.
Charon VI: 5dbc98dcc983a70728bd082d1a47546e
Charon VI: f72c915d8f575a5c0999b5f37b6d99b7
Charon VI: a20bba554bfa1580a9d4aa2b6879ed46
Charon VI: 02beeea47ee3cfe212e6bd843b9ce7d3
Charon VI: 3112c7a8b6cd1677db0e3173e140fc05
Charon VI: 50f4646135205fd4a5417e460cf71d3c
Charon VI: eb22cfa0890a2df3177966854a7176bc
Charon VI: 845f49aa19c955b849d57593bf09d224
Charon VI: 87f63931da79aa969ac4a776ce6cfb03
Charon VI: 9793d9d6041c80f46ad7c1f530c8bbf8
Charon VI: 2f88d89a8f50426a6285449be3286708
Charon VI: 61bd22f017588208a0cacdf9a1a7ca1e
Charon VI: a7623c8b76316e10538782371b709415
Charon VI: c6cca42180caba17e9e6882dc66cc6ee
Charon VI: 7c854900e46ebc5ee5680032b3e334de
Charon VI: ac81882b848b7673d73777ca22908c0d
Charon VI: 4ce97d67963edca55cdd21d46a68f5bb
Charon VI: 4abb62a00bccb775321f2720f2c7750b
Charon VI: 67e00e8ef738fe75afdb42b22e50371e
Charon VI: b561052e5697ee5f1491b5e350fb78e1
Charon VI: That's all.
R1kS: Wow, that's a lot of them! I'll see what I can do.
Charon VI: You are on your own. I feel like someone is listening to us right now. We've never met, bye!
R1kS: Yeah, I feel the same. Even this channel ain't secure no more. Bye!
```

Only 33 out of them are 'usable' as the every other is a confirmation (OK)

We can use a MD5 online cracker to find the password for the zip file (it is the only encrypted file)



CrackStation
CrackStation ≫ Password Hashing Security ≫ Defuse Security ≫

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

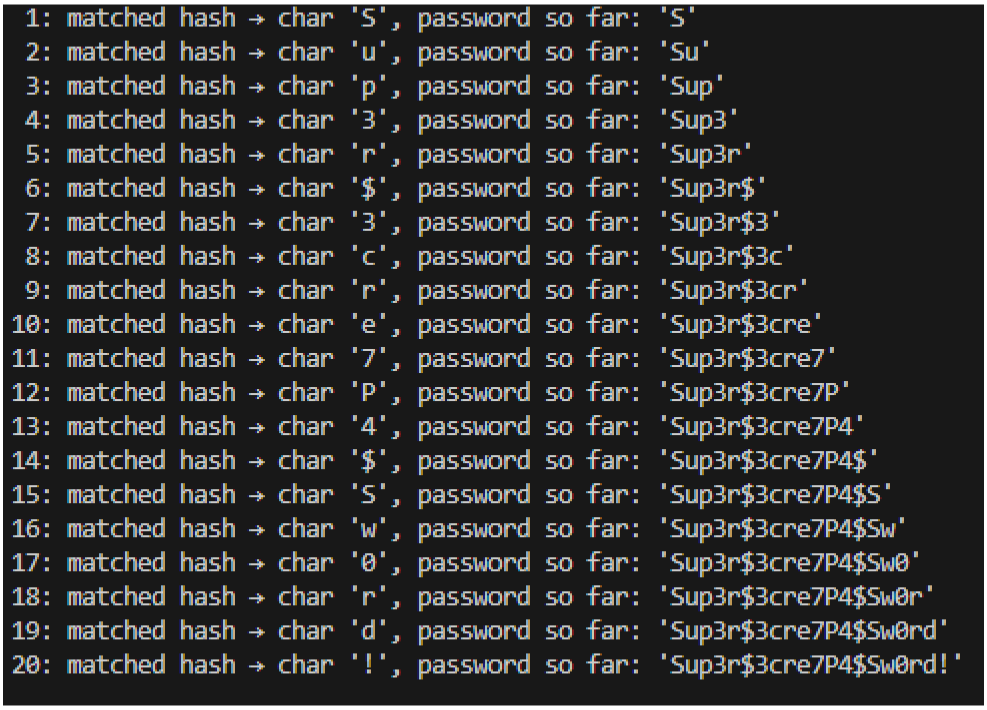
```
3112c7a8b6cd1677db0e3173e140fc05
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
3112c7a8b6cd1677db0e3173e140fc05	md5	Sup3r

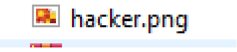
After this one we can construct a minimal Python script to get the other ones (GPT can help us here)

```python
#!/usr/bin/env python3
import hashlib
import string
#1) Hashes are pasted here
raw_hashes = """
5dbc98dcc983a70728bd082d1a47546e
f72c915d8f575a5c0999b5f37b6d99b7
a20bba554bfa1580a9d4aa2b6879ed46
02beeea47ee3cfe212e6bd843b9ce7d3
3112c7a8b6cd1677db0e3173e140fc05
50f4646135205fd4a5417e460cf71d3c
eb22cfa0890a2df3177966854a7176bc
845f49aa19c955b849d57593bf09d224
87f63931da79aa969ac4a776ce6cfb03
9793d9d6041c80f46ad7c1f530c8bbf8
2f88d89a8f50426a6285449be3286708
61bd22f017588208a0cacdf9a1a7ca1e
a7623c8b76316e10538782371b709415
c6cca42180caba17e9e6882dc66cc6ee
7c854900e46ebc5ee5680032b3e334de
ac81882b848b7673d73777ca22908c0d
4ce97d67963edca55cdd21d46a68f5bb
4abb62a00bccb775321f2720f2c7750b
67e00e8ef738fe75afdb42b22e50371e
b561052e5697ee5f1491b5e350fb78e1
""".strip().splitlines()
  # 2) Clean up each hash
hashes = [h.strip().lower() for h in raw_hashes]
  # 3) Our candidate alphabet (tweak if your password uses symbols)
charset = string.ascii_letters + string.digits + string.punctuation
def md5hex(s: str) -> str:
    return hashlib.md5(s.encode('utf-8')).hexdigest()
password = ""
for index, target_hash in enumerate(hashes, start=1):
    found_char = None
    for c in charset:
        if md5hex(password + c) == target_hash:
            found_char = c
            password += c
            print(f"{index:2d}: matched hash → char '{c}', password so far: '{password}'")
            break
    if not found_char:
        print(f"⚠️  Couldn’t match hash #{index}: {target_hash}")
        print("   • Check for typos in your list, stray whitespace, or if your charset needs expanding.")
        # stop here or continue depending on your preference:
        raise SystemExit(1)
print("\n🎉 Full password recovered:", password)
```

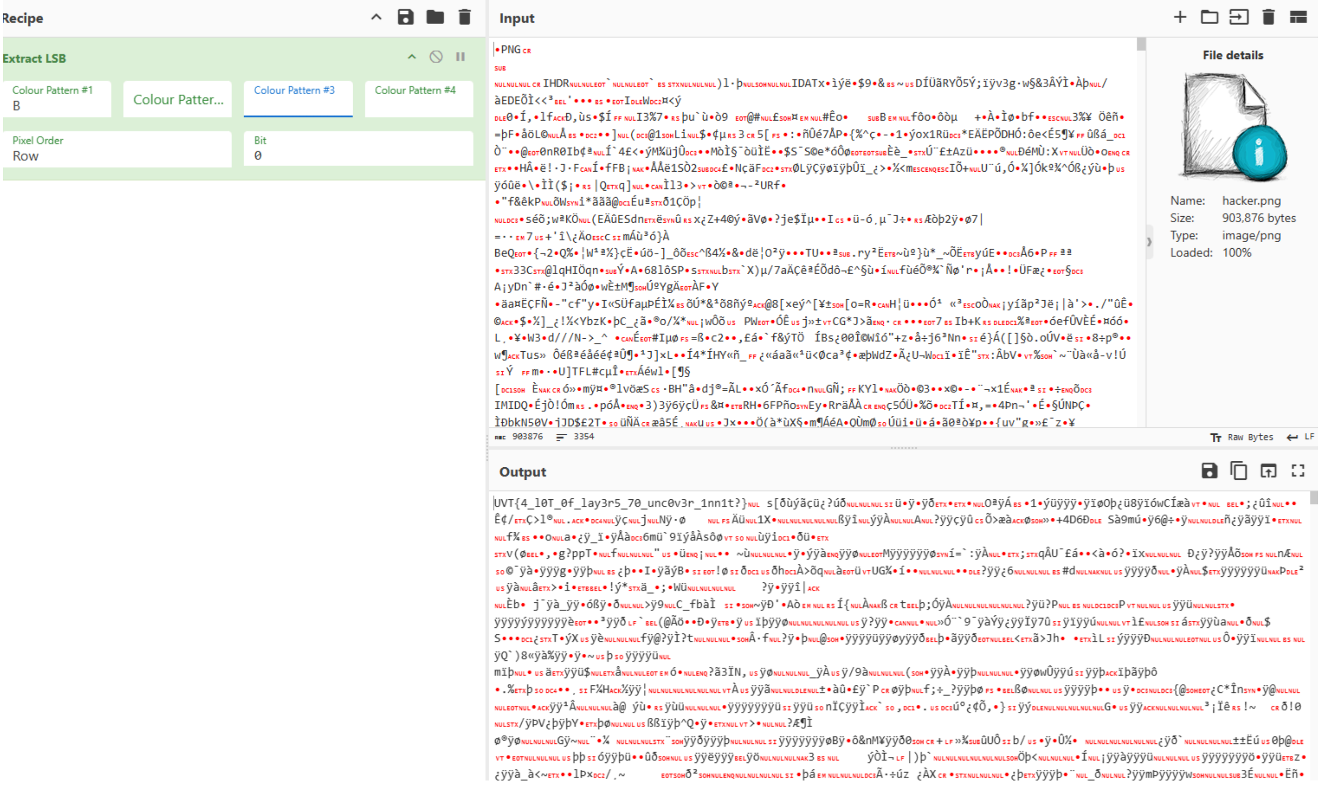


```
 1: matched hash → char 'S', password so far: 'S'
 2: matched hash → char 'u', password so far: 'Su'
 3: matched hash → char 'p', password so far: 'Sup'
 4: matched hash → char '3', password so far: 'Sup3'
 5: matched hash → char 'r', password so far: 'Sup3r'
 6: matched hash → char '$', password so far: 'Sup3r$'
 7: matched hash → char '3', password so far: 'Sup3r$3'
 8: matched hash → char 'c', password so far: 'Sup3r$3c'
 9: matched hash → char 'r', password so far: 'Sup3r$3cr'
10: matched hash → char 'e', password so far: 'Sup3r$3cre'
11: matched hash → char '7', password so far: 'Sup3r$3cre7'
12: matched hash → char 'P', password so far: 'Sup3r$3cre7P'
13: matched hash → char '4', password so far: 'Sup3r$3cre7P4'
14: matched hash → char '$', password so far: 'Sup3r$3cre7P4$'
15: matched hash → char 'S', password so far: 'Sup3r$3cre7P4$S'
16: matched hash → char 'w', password so far: 'Sup3r$3cre7P4$Sw'
17: matched hash → char '0', password so far: 'Sup3r$3cre7P4$Sw0'
18: matched hash → char 'r', password so far: 'Sup3r$3cre7P4$Sw0r'
19: matched hash → char 'd', password so far: 'Sup3r$3cre7P4$Sw0rd'
20: matched hash → char '!', password so far: 'Sup3r$3cre7P4$Sw0rd!'
```

After we decrypt the zip with the password `Sup3r$3cre7P4$Sw0rd!` , we get an image:



And by putting it into Cyberchef and extracting LSB we get the flag.



Extract LSB

Colour Pattern #1: B

Colour Patter...

Colour Pattern #3

Colour Pattern #4

Pixel Order: Row

Bit: 0

```
PNG
IHDR ... IDAT
```

903876   3354

Name: hacker.png
Size: 903,876 bytes
Type: image/png
Loaded: 100%

Raw Bytes   LF

```
UVT{4_l0T_0f_lay3r5_70_unc0v3r_1nn1t?}
```