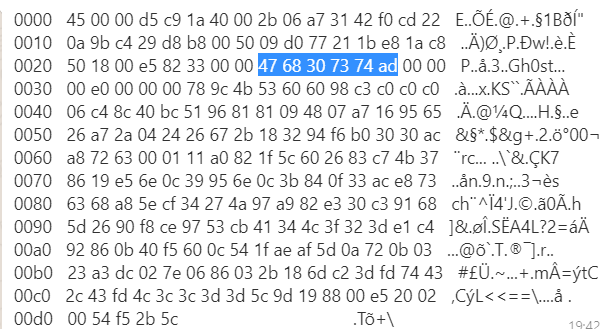
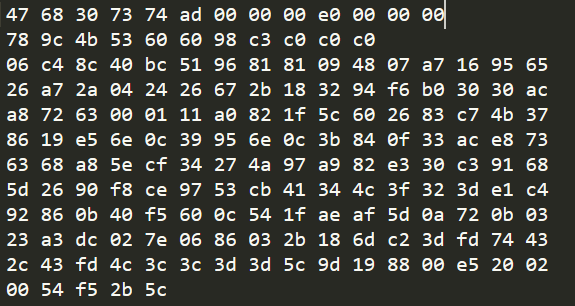
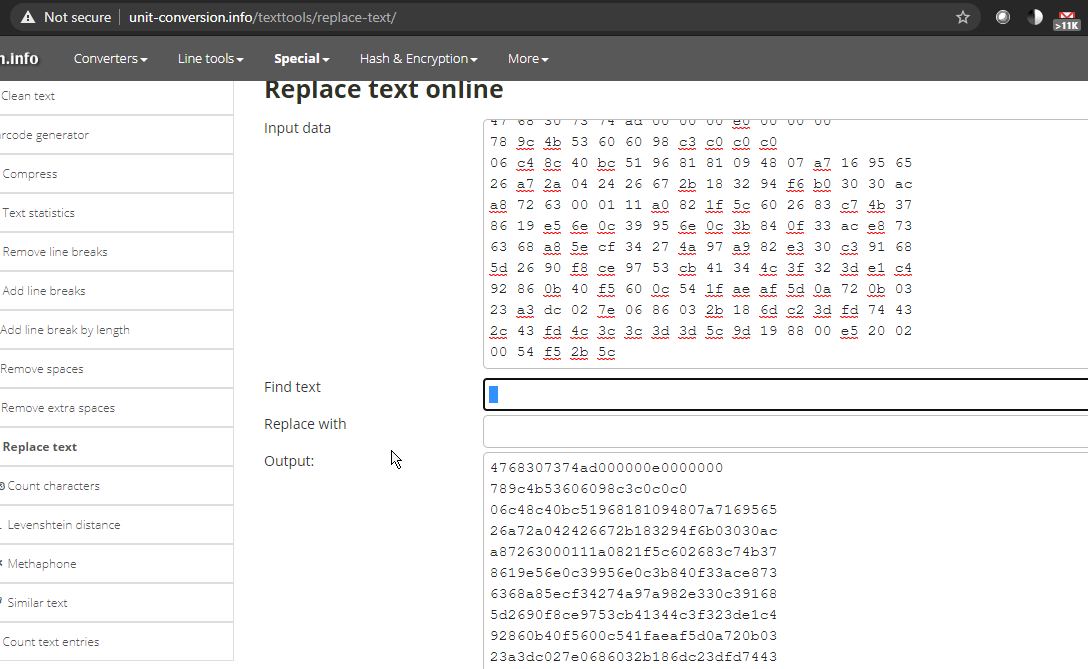
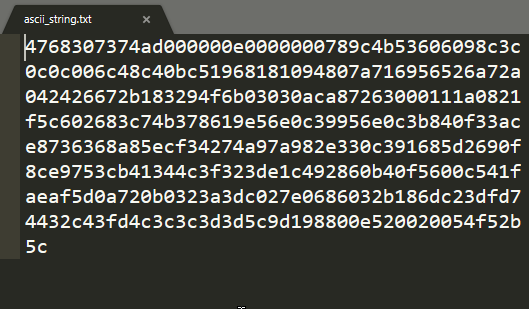
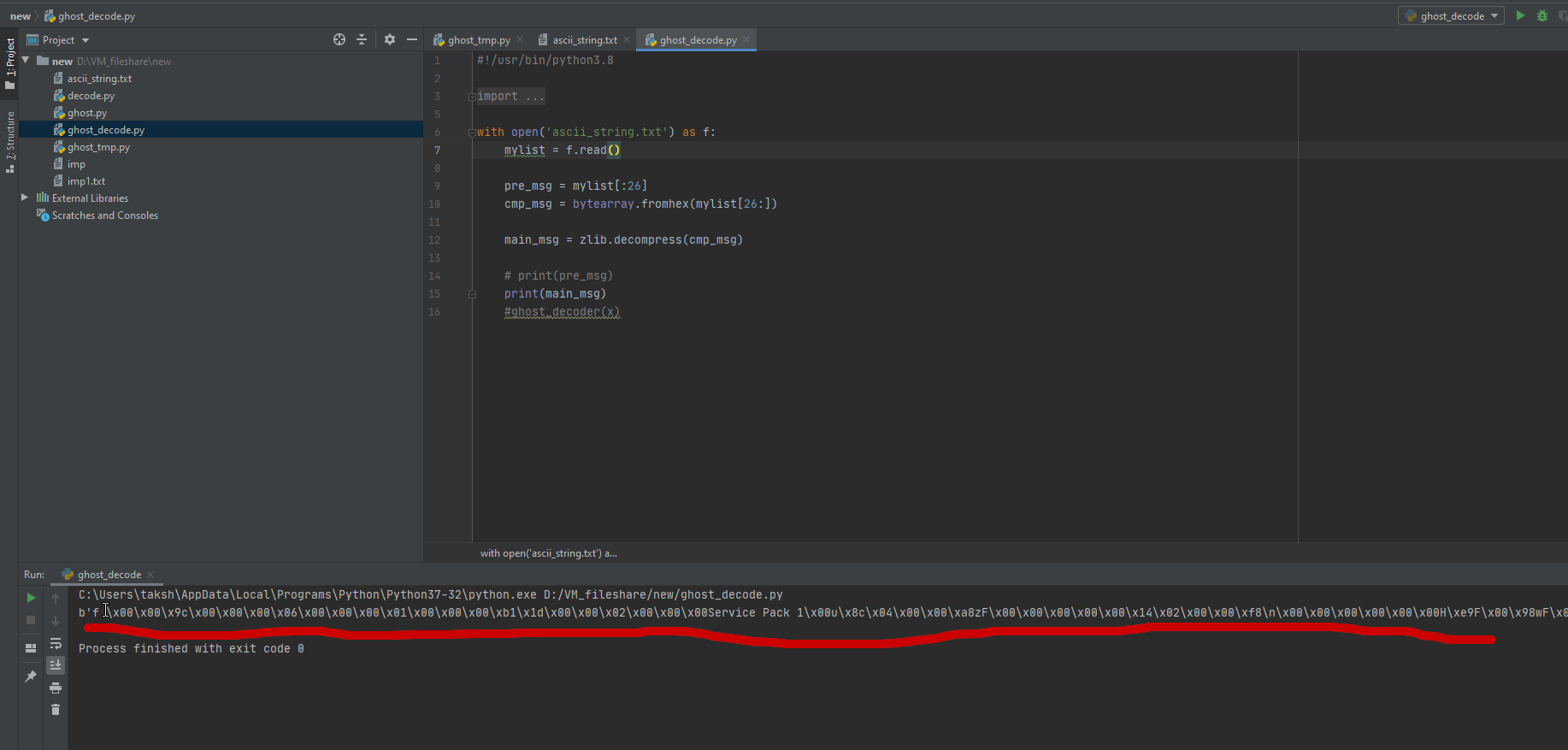
1. Copy only the hex bytes of network traffic to a new file say “ascii\_string”.
   1. 
   2. The data to be saved will start from “47 68 30 73 ad” == “Gh0st”, and end till the ending byte “54 f5 2b 5c”.
   3. 
   4. Next we need to remove all spaces in this file “ “.
      1. <http://www.unit-conversion.info/texttools/replace-text/>
      2. First remove whitespaces.
      3. Next we need to remove all new line.
      4. 
2. Now we need to input the file to ghost\_decode.py and run “ghost\_decode.py”

#!/usr/bin/python3.8  
  
import zlib  
  
with open('ascii\_string.txt') as f:  
 mylist = f.read()  
 pre\_msg = mylist[:26]  
 cmp\_msg = bytearray.fromhex(mylist[26:])  
 main\_msg = zlib.decompress(cmp\_msg)  
 print(main\_msg)

Executing the code we get the below output.



Now finding useful information from the output string,

\x00\x00\x9c\x00\x00\x00\x06\x00\x00\x00\x01\x00\x00\x00\xb1\x1d\x00\x00\x02\x00\x00\x00Service Pack 1\x00u\x8c\x04\x00\x00\xa8zF\x00\x00\x00\x00\x00\x14\x02\x00\x00\xf8\n\x00\x00\x00\x00\x00\x00H\xe9F\x00\x98wF\x00lyF\x00\xb8\x13\xc3\x00\xa8\x8eF\x00\x80{\xaf\x02\x9cZ-\x02x\x08\xc3\x00\xc4[-\x02\xb8\x13\xc3\x00\xb9\xe9\x95w\xb8\x13\xc3\x00\x00\x00\x00\x00\x14\x02\x00\x00\x00\x00\x00\x00\x14\x02\x00\x00\x00\x00\x00\x00\x90\xc8\xa4\x80\xd0Z-\x02\xd0Z-\x02\xd0[-\x02W/+u\x01\x00\x00\x00\x00\x01\x01\x1e\xa0\x0f\x00\x00\xc0\xa8\x01<WIN-T9UN4HIIHEC\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00w\x00\x00\x00\x00

\x00\x00\x00\x06 = Major version

\x00\x00\x00\x01 = Minor version

\xb1\x1d = Build number

Service Pack 1 = Service pack

\xa0\x0f = Speed

c0 = 192

a8 = 168

01 = 1

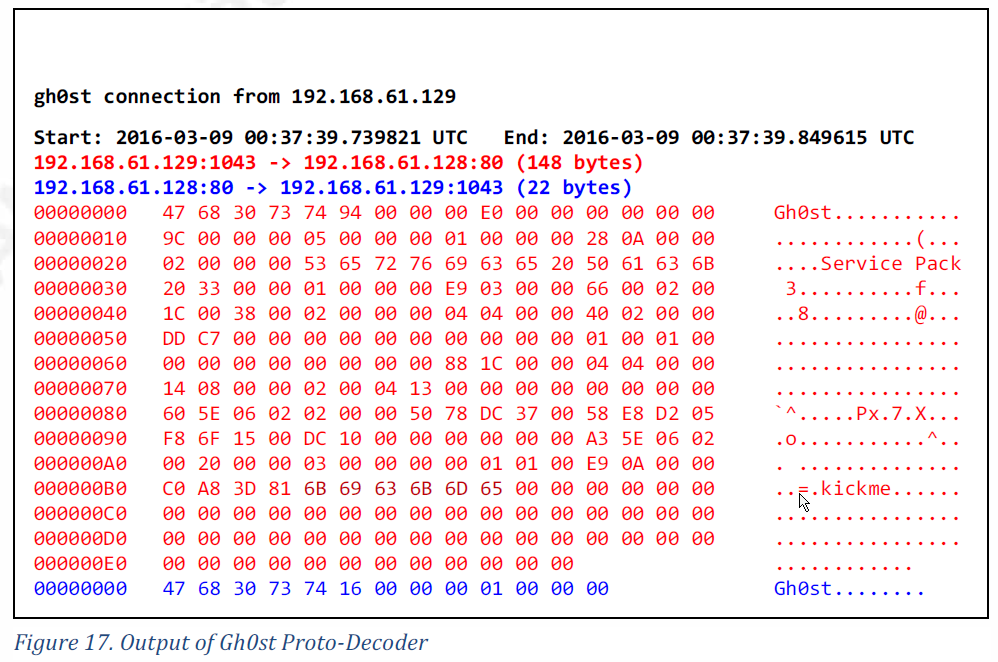
<(ASCII) = 3c(hex) = 60 (decimal)

IP = 192.168.1.60

WIN-T9UN4HIIHEC = hostname

Reference for the above information.

page = 20/51



page = 22/51

