Trivial Flag Transfer Protocol

Forensics

Description:

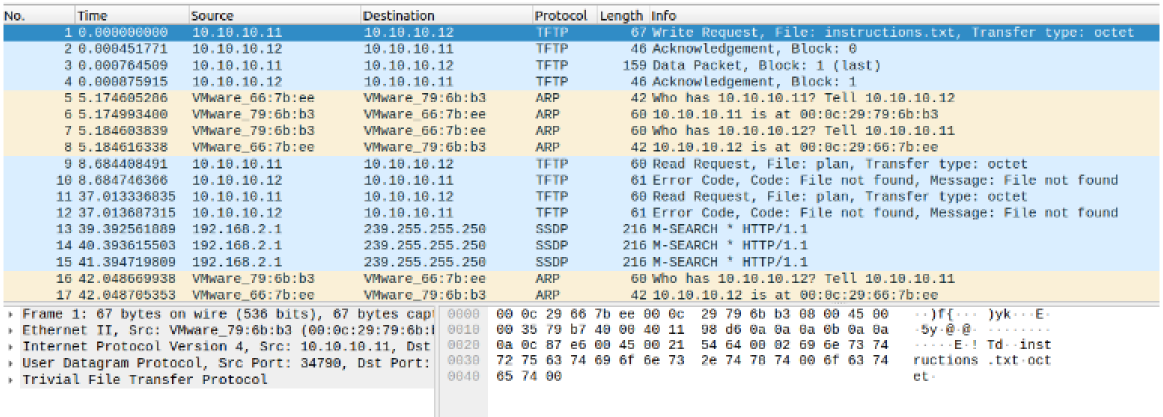
Figure out how they moved the flag.

Hints:

1) What are some other ways to hide data?

Solution:

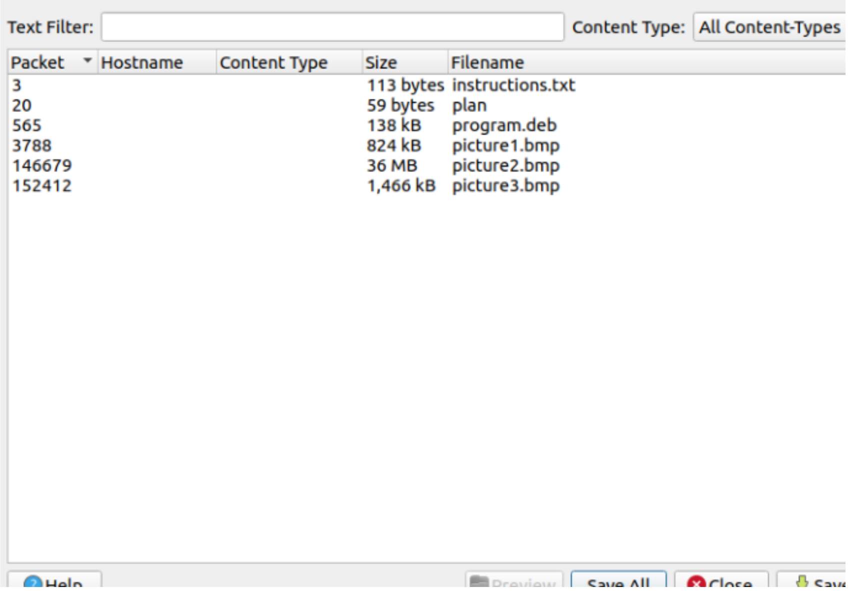
1) Open the file in wireshark to find out what it contains.



```
No.      Time          Source             Destination        Protocol Length Info
       1 0.000000000   10.10.10.11        10.10.10.12        TFTP       67 Write Request, File: instructions.txt, Transfer type: octet
       2 0.000451771   10.10.10.12        10.10.10.11        TFTP       46 Acknowledgement, Block: 0
       3 0.000764509   10.10.10.11        10.10.10.12        TFTP      159 Data Packet, Block: 1 (last)
       4 0.000875915   10.10.10.12        10.10.10.11        TFTP       46 Acknowledgement, Block: 1
       5 5.174605286   VMware_66:7b:ee    VMware_79:6b:b3    ARP        42 Who has 10.10.10.11? Tell 10.10.10.12
       6 5.174993400   VMware_79:6b:b3    VMware_66:7b:ee    ARP        60 10.10.10.11 is at 00:0c:29:79:6b:b3
       7 5.184603839   VMware_79:6b:b3    VMware_66:7b:ee    ARP        60 Who has 10.10.10.12? Tell 10.10.10.11
       8 5.184616338   VMware_66:7b:ee    VMware_79:6b:b3    ARP        42 10.10.10.12 is at 00:0c:29:66:7b:ee
       9 8.684408491   10.10.10.11        10.10.10.12        TFTP       60 Read Request, File: plan, Transfer type: octet
      10 8.684746366   10.10.10.12        10.10.10.11        TFTP       61 Error Code, Code: File not found, Message: File not found
      11 37.013336835  10.10.10.11        10.10.10.12        TFTP       60 Read Request, File: plan, Transfer type: octet
      12 37.013687315  10.10.10.12        10.10.10.11        TFTP       61 Error Code, Code: File not found, Message: File not found
      13 39.392561889  192.168.2.1        239.255.255.250    SSDP      216 M-SEARCH * HTTP/1.1
      14 40.393615503  192.168.2.1        239.255.255.250    SSDP      216 M-SEARCH * HTTP/1.1
      15 41.394719809  192.168.2.1        239.255.255.250    SSDP      216 M-SEARCH * HTTP/1.1
      16 42.048669938  VMware_79:6b:b3    VMware_66:7b:ee    ARP        60 Who has 10.10.10.12? Tell 10.10.10.11
      17 42.048705353  VMware_66:7b:ee    VMware_79:6b:b3    ARP        42 10.10.10.12 is at 00:0c:29:66:7b:ee
```

```
▸ Frame 1: 67 bytes on wire (536 bits), 67 bytes capt   0000  00 0c 29 66 7b ee 00 0c  29 79 6b b3 08 00 45 00   ··)f{··· )yk···E·
▸ Ethernet II, Src: VMware_79:6b:b3 (00:0c:29:79:6b:l   0010  00 35 79 b7 40 00 40 11  98 d6 0a 0a 0a 0b 0a 0a   ·5y·@·@· ········
▸ Internet Protocol Version 4, Src: 10.10.10.11, Dst    0020  0a 0c 87 e6 00 45 00 21  54 64 00 02 69 6e 73 74   ·····E·! Td··inst
▸ User Datagram Protocol, Src Port: 34790, Dst Port:    0030  72 75 63 74 69 6f 6e 73  2e 74 78 74 00 6f 63 74   ructions .txt·oct
▸ Trivial File Transfer Protocol                        0040  65 74 00                                           et·
```

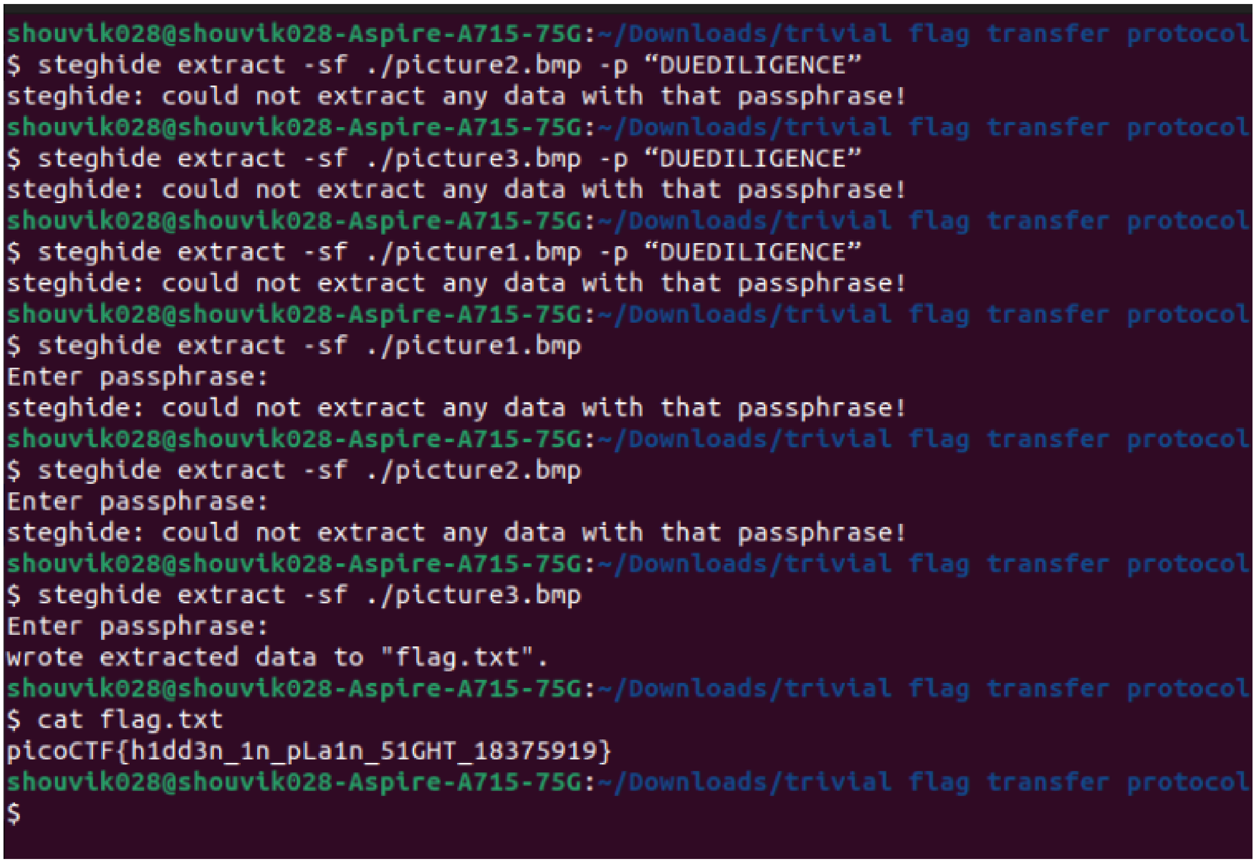
2) Use a filter to find what was sent and received.



Text Filter: Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
3			113 bytes	instructions.txt
20			59 bytes	plan
565			138 kB	program.deb
3788			824 kB	picture1.bmp
146679			36 MB	picture2.bmp
152412			1,466 kB	picture3.bmp

3) Use the cat command to find out what is contained in each file.
4) You will be given instructions to check out the photos and the password was DUEDILLIGENCE.
5) Use the command:
   steghide extract -sf <fiflename> -p <password>
   To obtain the flag.



```
shouvik028@shouvik028-Aspire-A715-75G:~/Downloads/trivial flag transfer protocol
$ steghide extract -sf ./picture2.bmp -p “DUEDILIGENCE”
steghide: could not extract any data with that passphrase!
shouvik028@shouvik028-Aspire-A715-75G:~/Downloads/trivial flag transfer protocol
$ steghide extract -sf ./picture3.bmp -p “DUEDILIGENCE”
steghide: could not extract any data with that passphrase!
shouvik028@shouvik028-Aspire-A715-75G:~/Downloads/trivial flag transfer protocol
$ steghide extract -sf ./picture1.bmp -p “DUEDILIGENCE”
steghide: could not extract any data with that passphrase!
shouvik028@shouvik028-Aspire-A715-75G:~/Downloads/trivial flag transfer protocol
$ steghide extract -sf ./picture1.bmp
Enter passphrase:
steghide: could not extract any data with that passphrase!
shouvik028@shouvik028-Aspire-A715-75G:~/Downloads/trivial flag transfer protocol
$ steghide extract -sf ./picture2.bmp
Enter passphrase:
steghide: could not extract any data with that passphrase!
shouvik028@shouvik028-Aspire-A715-75G:~/Downloads/trivial flag transfer protocol
$ steghide extract -sf ./picture3.bmp
Enter passphrase:
wrote extracted data to "flag.txt".
shouvik028@shouvik028-Aspire-A715-75G:~/Downloads/trivial flag transfer protocol
$ cat flag.txt
picoCTF{h1dd3n_1n_pLa1n_51GHT_18375919}
shouvik028@shouvik028-Aspire-A715-75G:~/Downloads/trivial flag transfer protocol
$
```

Flag: picoCTF{h1dd3n_1n_pLa1n_51GHT_18375919}