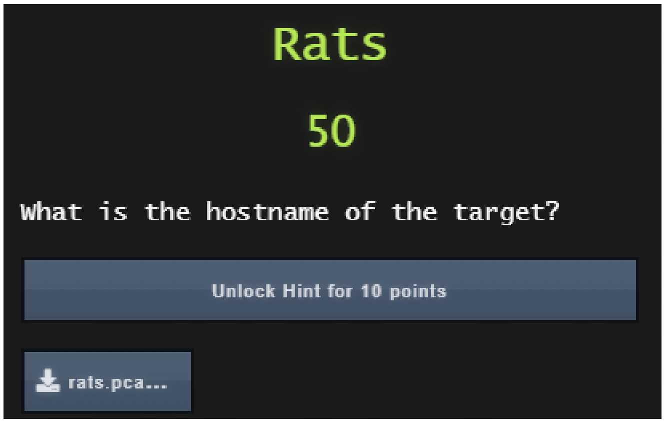
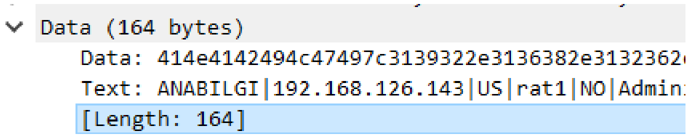


Rats

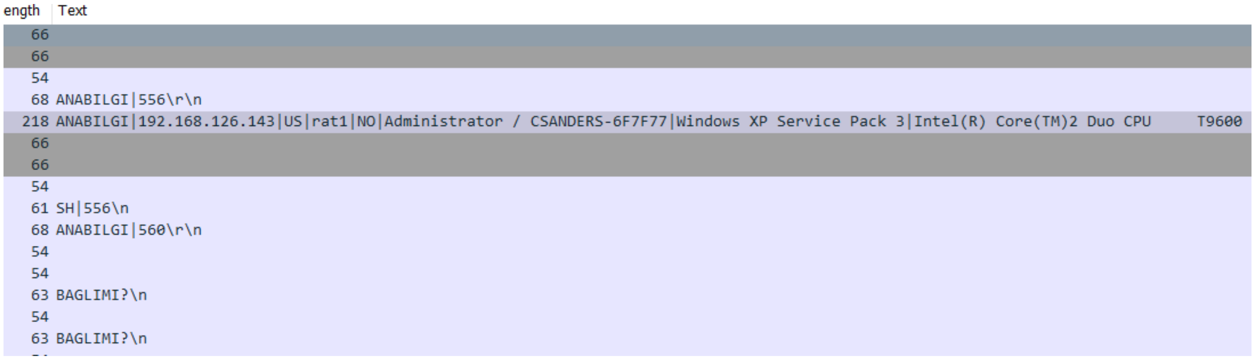
50

What is the hostname of the target?

If we look at some of the tcp packets they have a data section in them. We can add a column in wireshark to see the contents of these fields.



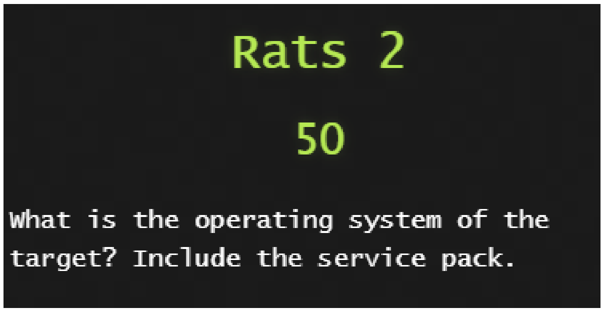
```
Data (164 bytes)
    Data: 414e4142494c47497c3139322e3136382e3132362
    Text: ANABILGI|192.168.126.143|US|rat1|NO|Admin
    [Length: 164]
```



```
ength  Text
   66
   66
   54
   68 ANABILGI|556\r\n
  218 ANABILGI|192.168.126.143|US|rat1|NO|Administrator / CSANDERS-6F7F77|Windows XP Service Pack 3|Intel(R) Core(TM)2 Duo CPU     T9600
   66
   66
   54
   61 SH|556\n
   68 ANABILGI|560\r\n
   54
   54
   63 BAGLIMI?\n
   54
   63 BAGLIMI?\n
```

We see the first few commands sent back to the attacker is system info.

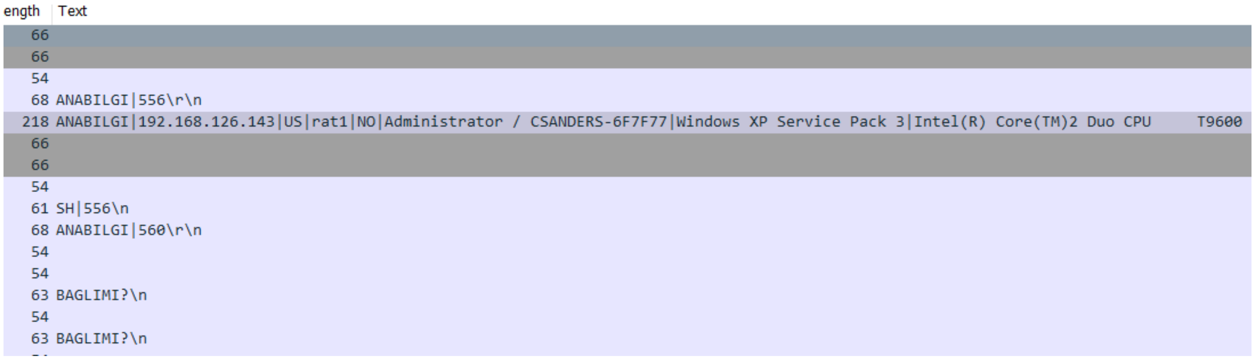
Flag: CSANDERS-6F7F77



Rats 2

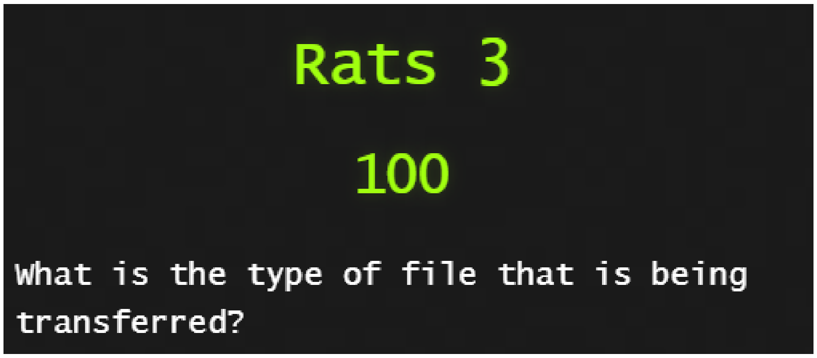
50

What is the operating system of the target? Include the service pack.



```
ength  Text
   66
   66
   54
   68 ANABILGI|556\r\n
  218 ANABILGI|192.168.126.143|US|rat1|NO|Administrator / CSANDERS-6F7F77|Windows XP Service Pack 3|Intel(R) Core(TM)2 Duo CPU     T9600
   66
   66
   54
   61 SH|556\n
   68 ANABILGI|560\r\n
   54
   54
   63 BAGLIMI?\n
   54
   63 BAGLIMI?\n
```

Flag: Windows XP Service Pack 3

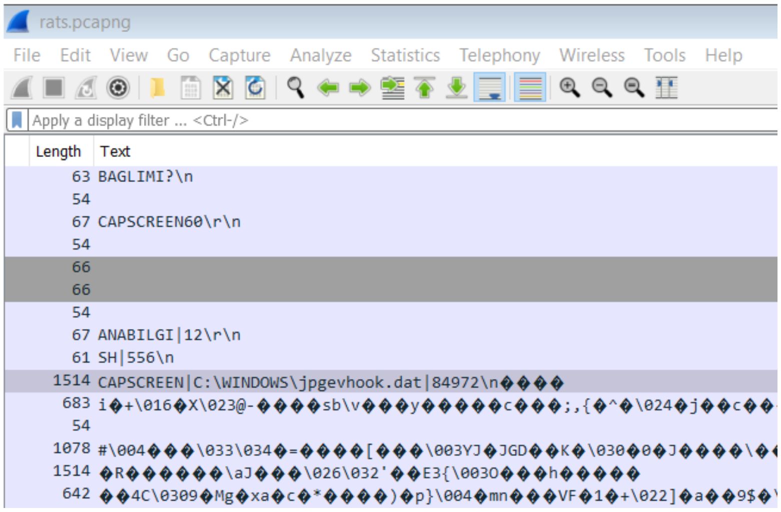


Rats 3

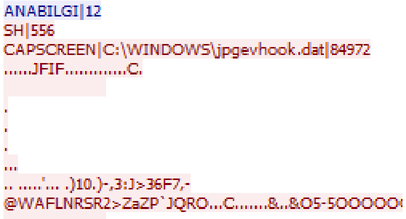
100

What is the type of file that is being transferred?

Scrolling down the text column we created we see the name of the file.



```
Length Text
    63 BAGLIMI?\n
    54
    67 CAPSCREEN60\r\n
    54
    66
    66
    54
    67 ANABILGI|12\r\n
    61 SH|556\n
  1514 CAPSCREEN|C:\WINDOWS\jpgevhook.dat|84972\n����
   683 i�+\016�X\023@-����sb\v���y������c���;,{�^�\024�j��c��
    54
  1078 #\004���\033\034�=����[���\003YJ�JGD��K�\030�0�J�����\�
  1514 �R�������\aJ���\026\032'��E3{\003O���h������
   642 ��4C\0309�Mg�xa�c�*�����)�p}\004�mn���VF�1�+\022]�a��9$�
```

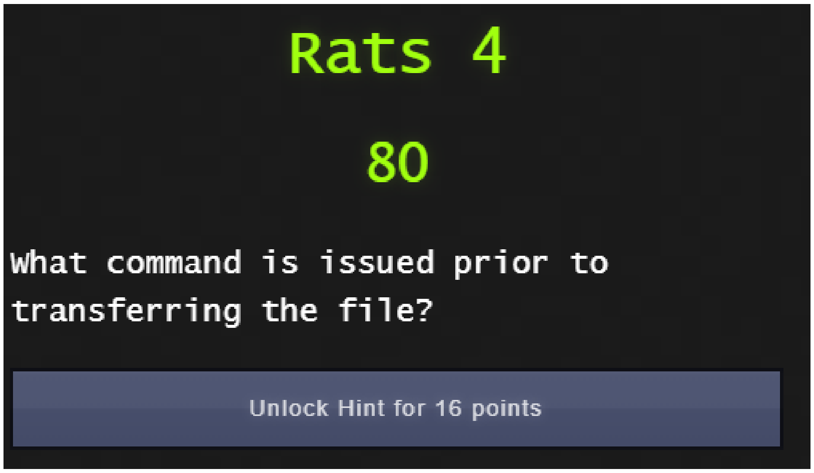


```
ANABILGI|12
SH|556
CAPSCREEN|C:\WINDOWS\jpgevhook.dat|84972
......JFIF..............C.

.
.
.
...
.. ......'... .)10.)-,3:J>36F7,-
@WAFLNRSR2>ZaZP`JQRO...C........&...&O5-5OOOOO
```

If we right click and follow that stream, we see the file is a JFIF which is another type of the common jpeg

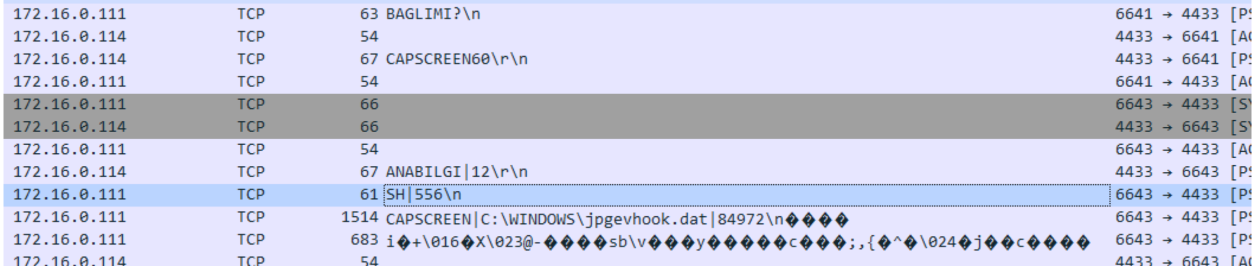
Flag: JPEG



Rats 4

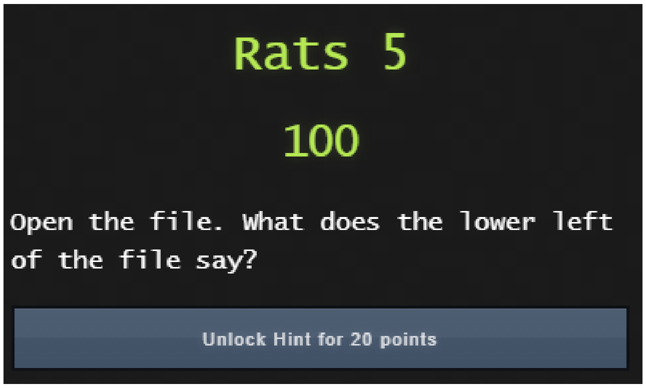
80

What command is issued prior to transferring the file?



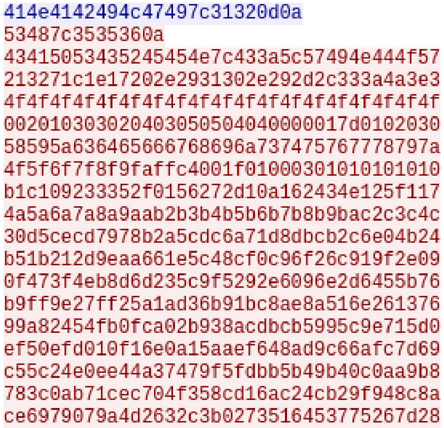
```
172.16.0.111    TCP      63 BAGLIMI?\n                                                  6641 → 4433 [P
172.16.0.114    TCP      54                                                             4433 → 6641 [A
172.16.0.114    TCP      67 CAPSCREEN60\r\n                                             4433 → 6641 [P
172.16.0.111    TCP      54                                                             6641 → 4433 [A
172.16.0.111    TCP      66                                                             6643 → 4433 [S
172.16.0.114    TCP      66                                                             4433 → 6643 [S
172.16.0.111    TCP      54                                                             6643 → 4433 [A
172.16.0.114    TCP      67 ANABILGI|12\r\n                                             4433 → 6643 [P
172.16.0.111    TCP      61 SH|556\n                                                    6643 → 4433 [P
172.16.0.111    TCP    1514 CAPSCREEN|C:\WINDOWS\jpgevhook.dat|84972\n����               6643 → 4433 [P
172.16.0.111    TCP     683 i�+\016�X\023@-����sb\v���y������c���;,{�^�\024�j��c����   6643 → 4433 [P
172.16.0.114    TCP      54                                                             4433 → 6643 [A
```

Flag: CAPSCREEN60

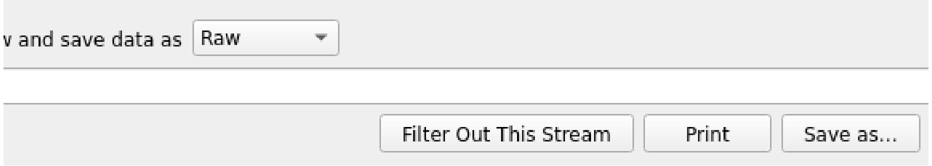


Open the file. What does the lower left of the file say?

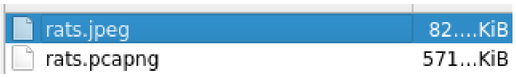
Carve the file out from the stream in Rats 3.



```
414e4142494c47497c31320d0a
53487c3535360a
434150534352454e7c433a5c57494e444f57
213271c1e17202e2931302e292d2c333a4a3e3
4f4f4f4f4f4f4f4f4f4f4f4f4f4f4f4f4f4f4f
0020103030204030505040400000017d0102030
58595a636465666768696a737475767778797a
4f5f6f7f8f9faffc4001f01000301010101010
b1c109233352f0156272d10a162434e125f117
4a5a6a7a8a9aab2b3b4b5b6b7b8b9bac2c3c4c
30d5cecd7978b2a5cdc6a71d8dbcb2c6e04b24
b51b212d9eaa661e5c48cf0c96f26c919f2e09
0f473f4eb8d6d235c9f5292e6096e2d6455b76
b9ff9e27ff25a1ad36b91bc8ae8a516e261376
99a82454fb0fca02b938acdbcb5995c9e715d0
ef50efd010f16e0a15aaef648ad9c66afc7d69
c55c24e0ee44a37479f5fdbb5b49b40c0aa9b8
783c0ab71cec704f358cd16ac24cb29f948c8a
ce6979079a4d2632c3b0273516453775267d28
```



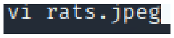
v and save data as Raw



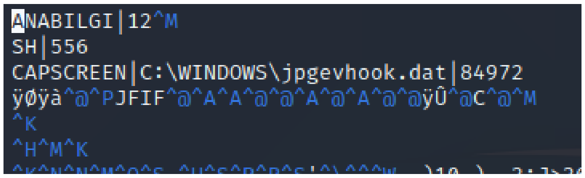
```
rats.jpeg      82....KiB
rats.pcapng    571...KiB
```

If you try to open the file you will get a corrupt file.

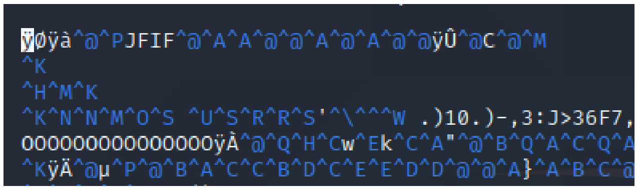
Remove the first three lines.



```
vi rats.jpeg
```

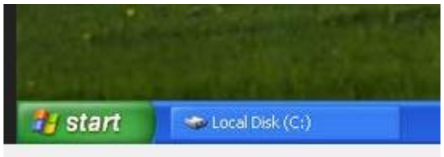


```
ANABILGI|12^M
SH|556
CAPSCREEN|C:\WINDOWS\jpgevhook.dat|84972
ÿØÿà^@^PJFIF^@^A^A^@^@^A^@^A^@^@ÿÛ^@C^@^M
^K
^H^M^K
```

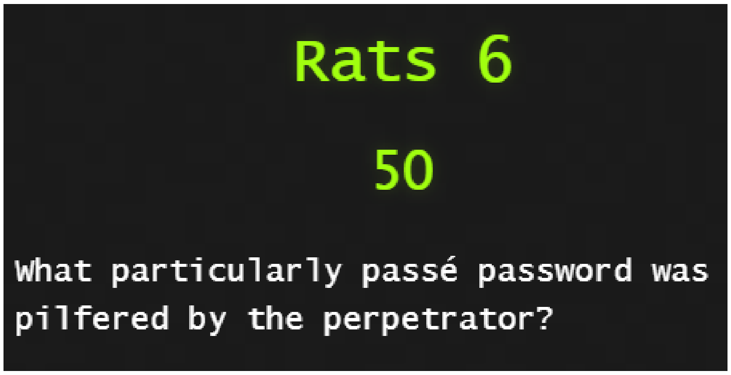


```
ÿØÿà^@^PJFIF^@^A^A^@^@^A^@^A^@^@ÿÛ^@C^@^M
^K
^H^M^K
^K^N^N^M^O^S ^U^S^R^R^S'^\^^^W .)10.)-,3:J>36F7,
OOOOOOOOOOOOOOOOÿÀ^@^Q^H^Cw^Ek^C^A"^@^B^Q^A^C^Q^A
^KÿÄ^@µ^P^@^B^A^C^C^B^D^C^E^E^D^D^@^@^A}^A^B^C^@
```

Open the screenshot



Flag: Start



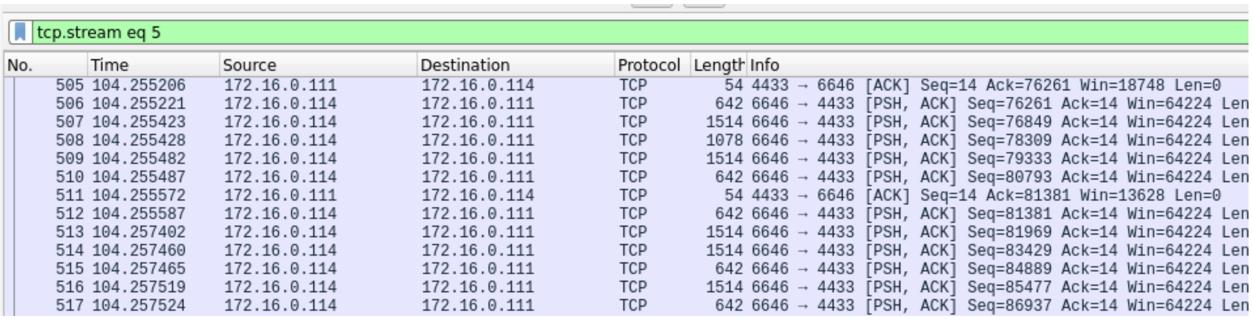
Rats 6

50

What particularly passé password was pilfered by the perpetrator?

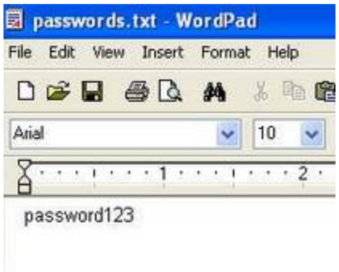
There are 7 streams in this pcap, and about 4-5 screenshots taken.

In stream 5, the screen capture gets the passwords.txt file opened.



```
tcp.stream eq 5
```

```
No.  Time        Source       Destination  Protocol Length Info
 505 104.255206  172.16.0.111 172.16.0.114 TCP        54 4433 → 6646 [ACK] Seq=14 Ack=76261 Win=18748 Len=0
 506 104.255221  172.16.0.114 172.16.0.111 TCP       642 6646 → 4433 [PSH, ACK] Seq=76261 Ack=14 Win=64224 Len
 507 104.255423  172.16.0.114 172.16.0.111 TCP      1514 6646 → 4433 [PSH, ACK] Seq=76849 Ack=14 Win=64224 Len
 508 104.255428  172.16.0.114 172.16.0.111 TCP      1078 6646 → 4433 [PSH, ACK] Seq=78309 Ack=14 Win=64224 Len
 509 104.255482  172.16.0.114 172.16.0.111 TCP      1514 6646 → 4433 [PSH, ACK] Seq=79333 Ack=14 Win=64224 Len
 510 104.255487  172.16.0.114 172.16.0.111 TCP       642 6646 → 4433 [PSH, ACK] Seq=80793 Ack=14 Win=64224 Len
 511 104.255572  172.16.0.111 172.16.0.114 TCP        54 4433 → 6646 [ACK] Seq=14 Ack=81381 Win=13628 Len=0
 512 104.255587  172.16.0.114 172.16.0.111 TCP       642 6646 → 4433 [PSH, ACK] Seq=81381 Ack=14 Win=64224 Len
 513 104.257402  172.16.0.114 172.16.0.111 TCP      1514 6646 → 4433 [PSH, ACK] Seq=81969 Ack=14 Win=64224 Len
 514 104.257460  172.16.0.114 172.16.0.111 TCP      1514 6646 → 4433 [PSH, ACK] Seq=83429 Ack=14 Win=64224 Len
 515 104.257465  172.16.0.114 172.16.0.111 TCP       642 6646 → 4433 [PSH, ACK] Seq=84889 Ack=14 Win=64224 Len
 516 104.257519  172.16.0.114 172.16.0.111 TCP      1514 6646 → 4433 [PSH, ACK] Seq=85477 Ack=14 Win=64224 Len
 517 104.257524  172.16.0.114 172.16.0.111 TCP       642 6646 → 4433 [PSH, ACK] Seq=86937 Ack=14 Win=64224 Len
```



password123

Flag: password123