Cyle Roberts
CS 485-01 Fall 2024
Encryption Assignment 1
September 12 2024

preconditions… I used the included logins.txt file and provided key/iv.

Step 1(ECB changed 1st bit):
1. The first 16 bytes were lost. The rest of the file was the same after the changes.
2. ECB is a block cipher that does not use any type of chaining. So only the block that was modified was affected.
3.

(altered ciphertext)

cipher.bin × logins.txt × decrypedECB.txt ×

```
00000000  BA 57 1D 05 BD C5 63 D0 65 39 31 73 A0 11 D0 1D  ||W..╝┼cлe91sá.╨.
00000010  C0 8F AC 70 57 B3 40 34 28 8B 38 60 90 BC 0E BA  └Å¼pW│@4(ï8`É╝.│
00000020  E4 23 9E 46 F2 9C 48 13 23 87 9F AA FC 6B 21 2D  Σ#₧F≥£H.#çƒ¬ⁿk!-
00000030  95 FE 24 19 7D 81 D6 0E DD 75 2F AF 88 11 C5 C0  ò•$.}üⁿ.▌u/»ê.┼└
00000040  97 DF 5D 95 43 2C 6A 30 8A D2 6E 4D 56 70 6A 10  ù▀]òC,j0è╥nMVpj.
00000050  FC B8 6C A7 11 B0 52 EB 93 C6 E7 96 3D A3 7D E7  ⁿ╕l°.\RδôΣτû=ú}τ
00000060  FE 40 65 61 0C 28 43 0B BB 30 E7 70 19 EE 6A 50  ▪@ea.(C.╗0τp.εjP
00000070  5F 65 71 3B 3D 56 A6 93 4B F7 2B 7F 7C D7 1C 22  _eq;=Vªô╬≈+⌂|╫."
00000080  F7 6E 2C 32 77 41 77 3D A1 67 8F C4 67 15 39 EA  ≈n,2wAw=íg╟─g.9Ω
00000090  1A FA 77 1A 76 53 44 31 97 48 9C BF 52 7B F0 A7  .·w.vSD1ùH£┐R{≡°
000000A0  AC 8E 9B 42 D5 48 03 33 30 3E 83 B4 00 17 2A 97  ¼Ä¢B╒H.30>â┤..*ù
000000B0  46 93 96 A7 49 BD 18 C4 62 C0 64 A5 0F 64 83 6C  Fôû°I╜.─b└dÑ.dâl
000000C0  F9 46 1C 14 9D 2C 8E EA 11 4F 71 0C 19 C9 3E C4  ·F..¥,ÄΩ.Oq..╔>─
000000D0  4F C2 49 3A 78 98 FE 15 33 A0 1C CB 84 F9 B5 91  O┬I:xÿ▪.3á.╦ä·╡æ
000000E0  36 4A BB 15 85 BB 14 AA 3C 59 C4 7B A6 E5 07 6D  6J╗.à╗.¬<Y─{ªσ.m
000000F0  68 30 D6 80 1A BF 42 56 27 DF 2C 43 0B D5 2D 7F  h0╓Ç.┐BV'▀,C.╒⁻⌂
00000100  61 D0 5B 10 A0 3F 63 C0 CC CE 31 ED 51 F5 10 06  aлá?c└╠╬1φQ⌡..
00000110  A9 4E 30 CF 6F 72 85 46 35 20 5C 03 AB 7A A6 20  ⌐N0╧oràF5 \.½zª
00000120  AA 56 29 94 5D EE 88 B7 56 62 0D 3A 23 C0 42 2E  ¬V)ö]εê╖Vb.:#└B.
00000130  85 2E 7A 69 55 0C FD 95 44 1E F0 77 19 02 C0 AC  à.ziU.²òD.≡w..└¼
00000140  AE 7F C6 EA 04 EA B1 4D 2D 41 F4 44 9C 0A E9 4E  «⌂╞Ω.Ω▒M-A⌠D£.ΘN
00000150  68 32 44 F2 E4 9F CE 2F DE 9C AC 2E 75 1C 9E 9D  h2D≥Σƒ╬/▐£¼.u.₧¥
00000160  42 C9 51 FD B1 8B 6E 6F 20 BA B7 46 B6 6E 1A 17  B╔Q²▒ïno ╖┐F╢n..
00000170  30 63 04 C7 68 42 3D 8F CD 63 3D A7 32 E6 A3 D8  0c.╟hB=Å═c=°2µú╪
00000180  0C 38 93 11 2A 8D 1E 8D 05 04 AC 60 9B D7 3E 35  .8ô.*ì.ì..¼`¢╫>5
00000190  86 4F 80 FF 2D 13 F0 12 C1 B2 AB 27 AA ED 9A ED  åOÇ -.≡.┴▓½'¬φÜφ
000001A0  99 C0 F1 16 C5 FC 69 47 67 D5 C9 C2 46 AC 62 F1  Ö└±.┼ⁿiGg╒╔╥F¼b±
000001B0  76 C4 16 7A C6 8C 96 F5 69 18 D6 00 92 8B 53 F6  v─.z╞îûij.╓.ÆïS÷
000001C0  4A C7 A4 22 DC C1 E8 17 80 C6 DE 40 AF 80 56 12  J╟ñ"▄┴Φ.Ç╞▌@»ÇV.
000001D0  50 AF CB 9C EB 40 29 B7 2B 8A 85 A6 9F F4 81 8C  P»╦£δ@)╖+èàªƒ⌠üî
000001E0  97 27 82 66 25 42 61 B7 7F 29 50 6D 2E 13 C2 7C  ù'éf%Ba╖⌂)Pm..┬|
000001F0  32 52 57 A7 23 FD 63 63 F0 4D 0E 74 21 97 1A 43  2RW°#²cc≡M.t!ù.C
00000200  05 8A CF FD A5 64 83 79 B2 F3 D4 EC 49 5C BA 7E  .è┴²Ñdây▒≤└∞I\╟~
00000210  C7 33 2D 58 50 88 55 E7 81 0F DB 3B F2 29 C9 1E  ╟3-XPêUτü.▌;≥)╓.
00000220  7B A4 42 6A E0 74 81 84 24 96 31 13 BA 09 B2 FA  {ñBjατüä$û1.╟.▒·
00000230  BB FC C9 A5 2E CF 1E 05 42 88 43 CE C5 B0 8F 26  ╗ⁿ╓Ñ.╧..BêC╬┼\Å&
00000240  C4 24 65 D1 E4 95 E9 87 67 62 F7 8A E4 0A 99 AD  ─$e╤Σò0çgb≈èΣ.Ö¡
00000250  95 7F CB 2F 4C E7 C9 C4 C7 C6 EC 8E 9D 47 C3 DC  ò⌂╦/Lτ╔─╟╞∞Ä¥G├▄
00000260  6B 56 5A 88 A8 89 F2 6F 08 15 84 A5 E4 AB B3 2D  kVZê¿ë≥o..äÑΣ½│-
00000270  B0 44 6B F7 02 DE C6 A9 77 37 12 01 C5 1E EC 99  \Dk≈.▌╞╌w7..┼.∞Ö
00000280  F3 CC F9 F1 84 22 F0 21 C0 C8 40 58 C9 1A E9 E4  ≤╠╬·±ä"≡!└╚@X╔.0Σ
00000290  C7 8A 27 E1 FB 70 F7 C4 34 84 4E 4D 37 C8 90 FC  ╟è'ß√p≈─4äNM7╚Én
000002A0  75 20 7B 99 35 76 5B F2 32 4C 2B D6 2C 90 6B 23  u {Ö5v[≥2L+╓,Ék#
000002B0  EA FC 7F 52 49 0E F0 C3 3A C7 0F F7 CB 24 0E 08  Ωⁿ⌂RI.≡├:╟.≈╦$..
```

(After decryption)

cipher.bin × logins.txt × decrypedECB.txt ×

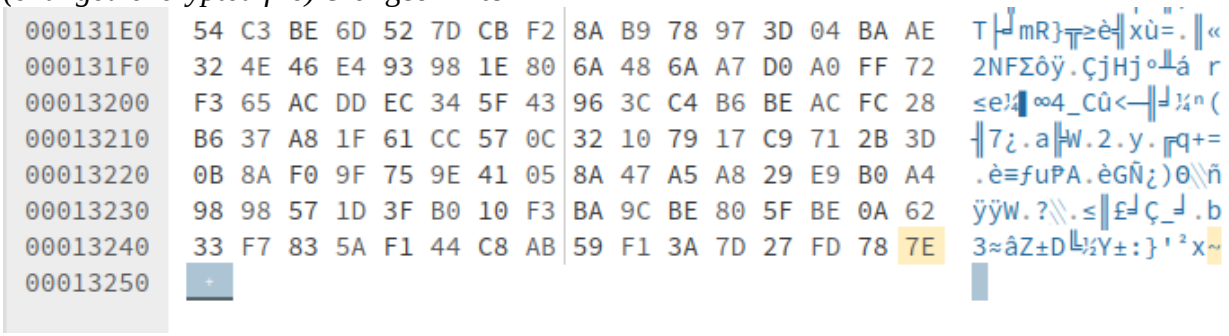
```
00000000  6A A2 D6 F2 27 E4 BE 21  89 78 04 A6 52 BF 5A 45  jó╥≥'Σ╛!ëx.ªR┐ZE
00000010  74 79 20 20 20 20 31 39  35 2E 32 31 39 2E 31 36  ty    195.219.16
00000020  36 2E 35 33 20 20 20 54  75 65 20 53 65 70 20 32  6.53   Tue Sep 2
00000030  36 20 30 32 3A 35 31 20  2D 20 30 32 3A 35 31 20  6 02:51 - 02:51
00000040  20 28 30 30 3A 30 30 29  0A 61 64 6D 69 6E 20 20   (00:00).admin
00000050  20 20 73 73 68 3A 6E 6F  74 74 79 20 20 20 20 31    ssh:notty    1
00000060  39 35 2E 32 31 39 2E 31  36 36 2E 35 33 20 20 20  95.219.166.53
00000070  54 75 65 20 53 65 70 20  32 36 20 30 32 3A 35 31  Tue Sep 26 02:51
00000080  20 2D 20 30 32 3A 35 31  20 20 28 30 30 3A 30 30   - 02:51  (00:00
00000090  29 0A 61 64 6D 69 6E 20  20 20 20 73 73 68 3A 6E  ).admin    ssh:n
000000A0  6F 74 74 79 20 20 20 20  31 30 34 2E 32 32 33 2E  otty    104.223.
000000B0  31 32 33 2E 39 38 20 20  20 54 75 65 20 53 65 70  123.98   Tue Sep
000000C0  20 32 36 20 30 32 3A 35  31 20 2D 20 30 32 3A 35   26 02:51 - 02:5
000000D0  31 20 20 28 30 30 3A 30  30 29 0A 61 64 6D 69 6E  1  (00:00).admin
000000E0  20 20 20 20 73 73 68 3A  6E 6F 74 74 79 20 20 20      ssh:notty
000000F0  20 31 30 34 2E 32 32 33  2E 31 32 33 2E 39 38 20   104.223.123.98
00000100  20 20 54 75 65 20 53 65  70 20 32 36 20 30 32 3A    Tue Sep 26 02:
00000110  35 31 20 2D 20 30 32 3A  35 31 20 20 28 30 30 3A  51 - 02:51  (00:
00000120  30 30 29 0A 61 64 6D 69  6E 20 20 20 20 73 73 68  00).admin    ssh
00000130  3A 6E 6F 74 74 79 20 20  20 20 31 39 32 2E 34 32  :notty    192.42
00000140  2E 31 31 36 2E 31 36 20  20 20 20 54 75 65 20 53  .116.16    Tue S
00000150  65 70 20 32 36 20 30 32  3A 35 31 20 2D 20 30 32  ep 26 02:51 - 02
00000160  3A 35 31 20 20 28 30 30  3A 30 30 29 0A 61 64 6D  :51  (00:00).adm
00000170  69 6E 20 20 20 20 73 73  68 3A 6E 6F 74 74 79 20  in    ssh:notty
00000180  20 20 20 31 39 32 2E 34  32 2E 31 31 36 2E 31 36     192.42.116.16
00000190  20 20 20 20 54 75 65 20  53 65 70 20 32 36 20 30      Tue Sep 26 0
000001A0  32 3A 35 31 20 2D 20 30  32 3A 35 31 20 20 28 30  2:51 - 02:51  (0
000001B0  30 3A 30 30 29 0A 70 69  20 20 20 20 20 20 20 73  0:00).pi       s
000001C0  73 68 3A 6E 6F 74 74 79  20 20 20 20 31 33 36 2E  sh:notty    136.
000001D0  33 32 2E 32 31 38 2E 31  36 30 20 20 20 4D 6F 6E  32.218.160   Mon
000001E0  20 53 65 70 20 32 35 20  31 30 3A 31 34 20 2D 20   Sep 25 10:14 -
000001F0  31 30 3A 31 34 20 20 28  30 30 3A 30 30 29 0A 70  10:14  (00:00).p
00000200  69 20 20 20 20 20 20 20  73 73 68 3A 6E 6F 74 74  i       ssh:nott
00000210  79 20 20 20 20 31 33 36  2E 33 32 2E 32 31 38 2E  y    136.32.218.
00000220  31 36 30 20 20 20 4D 6F  6E 20 53 65 70 20 32 35  160   Mon Sep 25
00000230  20 31 30 3A 31 34 20 2D  20 31 30 3A 31 34 20 20   10:14 - 10:14
00000240  28 30 30 3A 30 30 29 0A  70 69 20 20 20 20 20 20  (00:00).pi
00000250  20 73 73 68 3A 6E 6F 74  74 79 20 20 20 20 31 33   ssh:notty    13
00000260  36 2E 33 32 2E 32 31 38  2E 31 36 30 20 20 20 4D  6.32.218.160   M
00000270  6F 6E 20 53 65 70 20 32  35 20 31 30 3A 31 34 20  on Sep 25 10:14
00000280  2D 20 31 30 3A 31 34 20  20 28 30 30 3A 30 30 29  - 10:14  (00:00)
00000290  0A 70 69 20 20 20 20 20  20 20 73 73 68 3A 6E 6F  .pi       ssh:no
000002A0  74 74 79 20 20 20 20 31  33 36 2E 33 32 2E 32 31  tty    136.32.21
000002B0  38 2E 31 36 30 20 20 20  4D 6F 6E 20 53 65 70 20  8.160   Mon Sep
```

Step 2(CBC 1st bit):
1. The first block was completely corrupted and part of the second block was completely corrupted.
2. Only 2 blocks are affected because the XOR operation uses the previous block of the cipher text. I did not change the 2nd block so the next XOR operation doesn't use text that has been changed.

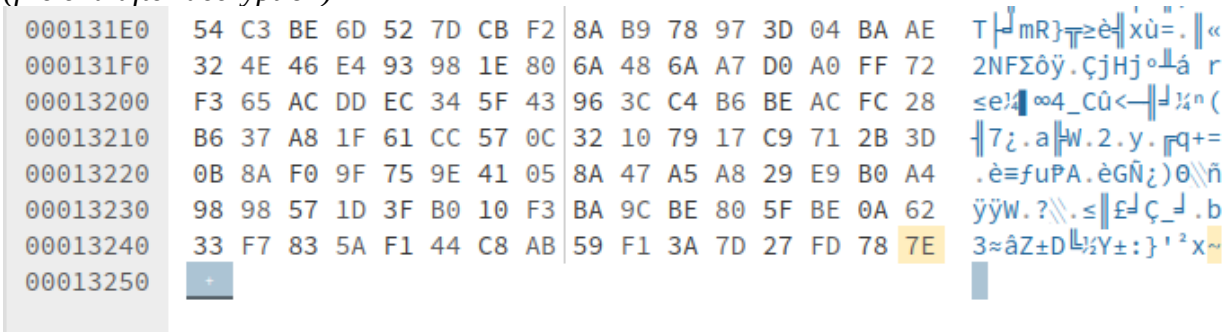
Step 3(CBC 129th bit):
1. The block containing 129th bit and also the next byte were corrupted. The rest of the data was fine.
2. For similar reasons to the previous step. It only affects the current block and xor operations in the next block that uses the bit that was changed were affected.

Step 4(CBC last bit):
1. All of the plain text was recovered besides last 2 bytes of plain text.
2. The last 2 bytes of data were blocked alone with padding so none of the other plain text was affected during the decryption. I did get an error message that said bad decryption.
3.

(changed encrypted file) changed 7F to 7E



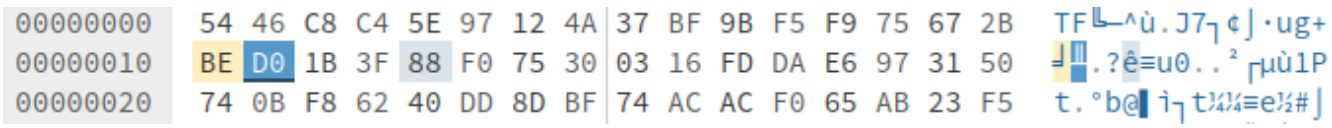
(file end after decryption)



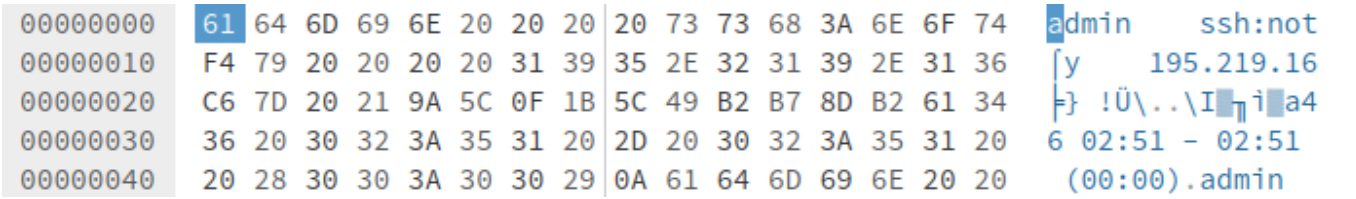
Step 5(CFB 1st bit):
1.It changed the first character and the 2nd block of characters. The rest of the text was not lost.
2. In CFB, the second block is dependent upon the previous block so since the first block was altered then the second block was completely changed. Only the first bit of the first block was changed because the IV was not changed and the rest of the block is not dependent upon the other bytes.

Step 6(CFB 129th bit):
1.The first block of data was unchanged and also 15 out of 16 bytes of data in the second block and the rest of the file was unchanged.
2. As the last step it was because the previous blocks are used for the IV for the next line of encryption. So only the next block and the singular byte that was changed are affected.
3.

(changed encrypted file) 3E to BE



(decrypted changed file)



```
00000000  61 64 6D 69 6E 20 20 20 20 73 73 68 3A 6E 6F 74   admin    ssh:not
00000010  F4 79 20 20 20 20 31 39 35 2E 32 31 39 2E 31 36   ⌠y    195.219.16
00000020  C6 7D 20 21 9A 5C 0F 1B 5C 49 B2 B7 8D B2 61 34   ╞} !Ü\..\I╖┐ì▒a4
00000030  36 20 30 32 3A 35 31 20 2D 20 30 32 3A 35 31 20   6 02:51 - 02:51
00000040  20 28 30 30 3A 30 30 29 0A 61 64 6D 69 6E 20 20    (00:00).admin
```

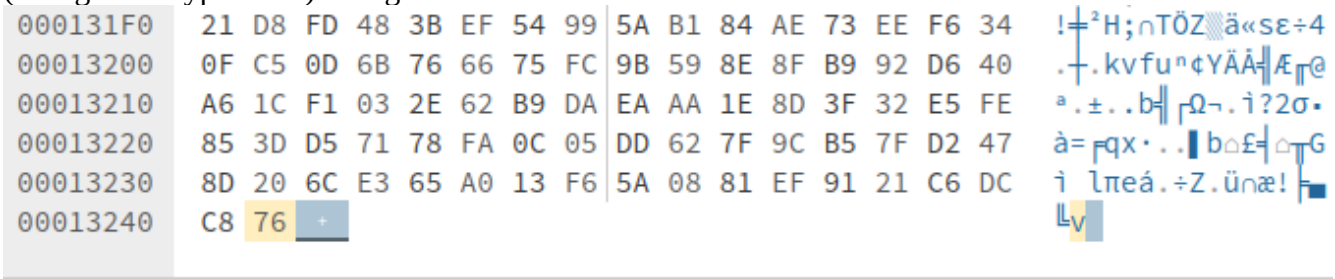
Step 7(CFB Last bit):
1. The end of line character was lost and the rest of the file was intact.
2. Like the last since there was not another line then it did not affect any character besides the last byte which represented the line feed character.

Step 8(OFB 1st bit):
1. Only the corresponding byte what contained the bit that was changed was affected and the rest of the file was the same as the file before encryption/decryption.
2. Since it acts for of a stream cipher then corresponding bits are changed.

Step 9(OFB 129th bit):
1. Only the corresponding byte what contained the bit that was changed was affected and the rest of the file was the same as the file before encryption/decryption.
2. Since it acts for of a stream cipher then corresponding bits are changed.

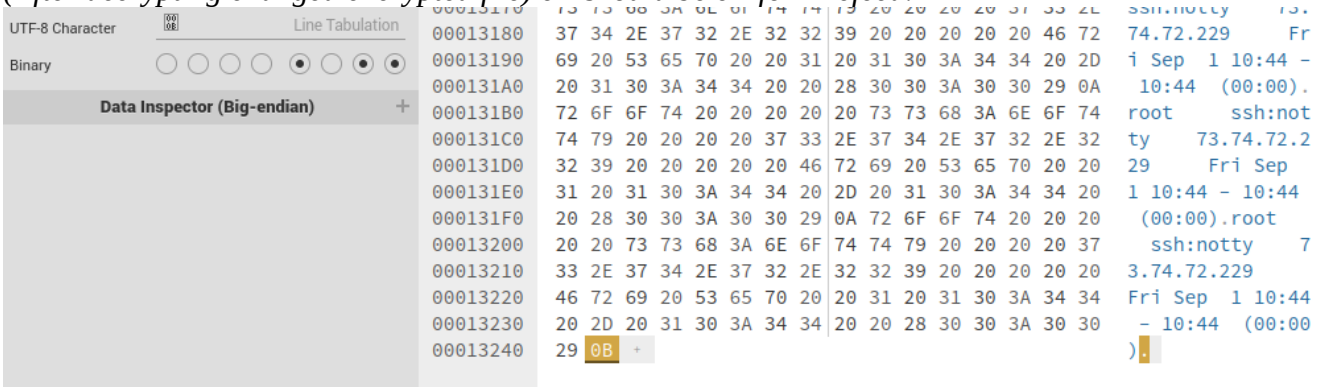
step 10(OFB last bit):
1. Only the last line feed was lost. The rest of the file was the same.
2. Since it acts for of a stream cipher then corresponding bits are changed.
3.

(changed encrypted file) changed from 77 to 76



```
000131F0  21 D8 FD 48 3B EF 54 99 5A B1 84 AE 73 EE F6 34   !╪²H;∩TÖZ▒ä«sε÷4
00013200  0F C5 0D 6B 76 66 75 FC 9B 59 8E 8F B9 92 D6 40   .┼.kvfuⁿ¢YÄÅ╣Æ╓@
00013210  A6 1C F1 03 2E 62 B9 DA EA AA 1E 8D 3F 32 E5 FE   ª.±..b╣ ┌Ω¬.ì?2σ▪
00013220  85 3D D5 71 78 FA 0C 05 DD 62 7F 9C B5 7F D2 47   à=╒qx·..▌b⌂£╡⌂╥G
00013230  8D 20 6C E3 65 A0 13 F6 5A 08 81 EF 91 21 C6 DC   ì lπeá.÷Z.ü∩æ!╞▄
00013240  C8 76                                             ╚v
```

(After decrypting changed encrypted file) 0B should be 0A for linefeed.




```
00013180  37 34 2E 37 32 2E 32 32 39 20 20 20 20 20 46 72   74.72.229     Fr
00013190  69 20 53 65 70 20 20 31 20 31 30 3A 34 34 20 2D   i Sep  1 10:44 -
000131A0  20 31 30 3A 34 34 20 20 28 30 30 3A 30 30 29 0A    10:44  (00:00).
000131B0  72 6F 6F 74 20 20 20 20 20 73 73 68 3A 6E 6F 74   root     ssh:not
000131C0  74 79 20 20 20 20 37 33 2E 37 34 2E 37 32 2E 32   ty    73.74.72.2
000131D0  32 39 20 20 20 20 20 46 72 69 20 53 65 70 20 20   29     Fri Sep
000131E0  31 20 31 30 3A 34 34 20 2D 20 31 30 3A 34 34 20   1 10:44 - 10:44
000131F0  20 28 30 30 3A 30 30 29 0A 72 6F 6F 74 20 20 20    (00:00).root
00013200  20 20 73 73 68 3A 6E 6F 74 74 79 20 20 20 20 37     ssh:notty    7
00013210  33 2E 37 34 2E 37 32 2E 32 32 39 20 20 20 20 20   3.74.72.229
00013220  46 72 69 20 53 65 70 20 20 31 20 31 30 3A 34 34   Fri Sep  1 10:44
00013230  20 2D 20 31 30 3A 34 34 20 20 28 30 30 3A 30 30    - 10:44  (00:00
00013240  29 0B                                            ).
```