

解析演習回答

回答です。

**授業で支持あるまでは
見ないことをお勧めします。**

TCPだけを表示すると、FTP通信している事がわかる。

capture010.pcapng

ファイル(E) 編集(E) 表示(V) 移動(G) キャプチャ(C) 分析(A) 統計(S) 電話(Y) 無線(W) ツール(I) ヘルプ(H)

tcp

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-------------|---------------|---------------|----------|--------|--|
| 45 | 7.788646473 | 192.168.10.12 | 192.168.10.14 | TCP | 78 | 57540 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 |
| 46 | 7.788682626 | 192.168.10.14 | 192.168.10.12 | TCP | 74 | 21 → 57540 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS= |
| 47 | 7.788988004 | 192.168.10.12 | 192.168.10.14 | TCP | 66 | 57540 → 21 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=6 |
| 48 | 7.790480599 | 192.168.10.14 | 192.168.10.12 | FTP | 86 | Response: 220 (vsFTPd 3.0.3) |
| 49 | 7.790829405 | 192.168.10.12 | 192.168.10.14 | TCP | 66 | 57540 → 21 [ACK] Seq=1 Ack=21 Win=131712 Len=0 TSval= |
| 50 | 7.791164314 | 192.168.10.12 | 192.168.10.14 | FTP | 72 | Request: FEAT |
| 51 | 7.791179053 | 192.168.10.14 | 192.168.10.12 | TCP | 66 | 21 → 57540 [ACK] Seq=21 Ack=7 Win=65280 Len=0 TSval=1 |
| 52 | 7.791487644 | 192.168.10.14 | 192.168.10.12 | FTP | 81 | Response: 211-Features: |
| 53 | 7.791516478 | 192.168.10.14 | 192.168.10.12 | FTP | 87 | Response: EPRT |
| 54 | 7.791669297 | 192.168.10.14 | 192.168.10.12 | FTP | 110 | Response: PASV |
| 55 | 7.791970302 | 192.168.10.12 | 192.168.10.14 | TCP | 66 | 57540 → 21 [ACK] Seq=7 Ack=36 Win=131712 Len=0 TSval= |

Frame 102: 5067 bytes on wire (40536 bits), 5067 bytes captured (40536 bits) on interface eth0, id 0

Ethernet II, Src: PcsCompu_4c:14:d6 (08:00:27:4c:14:d6), Dst: Apple_1f:f8:80 (8c:85:90:1f:f8:80)

Internet Protocol Version 4, Src: 192.168.10.14, Dst: 192.168.10.12

Transmission Control Protocol, Src Port: 37900, Dst Port: 57541, Seq: 1, Ack: 1, Len: 5001

FTP Data (5001 bytes data)

[Setup frame: 95]

[Setup method: PASV]

[Command: RETR /home/kali/MGT202105/xac]

Command frame: 100

0000 8c 85 90 1f f8 80 08 00 27 4c 14 d6 08 00 45 08 'L...E.

0010 13 bd 0d d1 40 00 40 06 83 f7 c0 a8 0a 0e c0 a8 @.@.

0020 0a 0c 94 0c e0 c5 e0 9d 59 6d b0 32 40 11 80 18 Ym.2@...

0030 01 fe a9 1a 00 00 01 01 08 0a 06 8b 00 37 27 2d 7'.

0040 d8 a2 f1 0f a0 a9 e1 4f d5 f7 9f dd b3 b3 8e 8f 0

0050 df 12 68 c1 bf b1 0f 07 e5 56 c7 3b 80 49 20 f0 ..h..... V.;.I .

0060 9f 55 1e 49 5a 3f ec a1 5b 4c c5 50 53 21 50 24 ..U·IZ?.. [L·PS!P\$

0070 91 46 10 4a 9b 75 9d c5 6d b9 b2 f3 68 41 a4 31 ..F·J·u.. m...hA·1

0080 f7 3d 9e ac d0 56 91 c7 19 e3 65 3f 63 01 35 ae ..=...V... e?c·5·

0090 62 1f 6e d6 52 11 e7 41 68 ad 2f bf 39 2f de 7e b·n·R·A h·/·9/·~

00a0 a9 f6 33 c3 4f 6a fc f7 db f1 5b eb d3 4b 37 4b ..3·0j... [·K7K

Transmission Control Protocol: Protocol

パケット数: 195 · 表示: 113 (57.9%) プロファイル: Default

ftp-dataのみを表示すると、xaa,xab,xacという3つのファイルをダウンロードしていることがわかる。

The image shows a Wireshark network traffic capture titled 'capture010.pcapng'. The filter bar is set to 'ftp-data'. The packet list shows three packets (102, 127, 150) all from source 192.168.10.14 to destination 192.168.10.12, using the FTP-DA protocol. The packet details for packet 102 are expanded, showing Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (Seq: 1, Ack: 1, Len: 5001) layers. The FTP Data (5001 bytes data) is highlighted, with a link to 'Setup frame: 95'. The command is 'RETR /home/kali/MGT202105/xac'. The packet bytes panel shows the raw data in hexadecimal and ASCII.

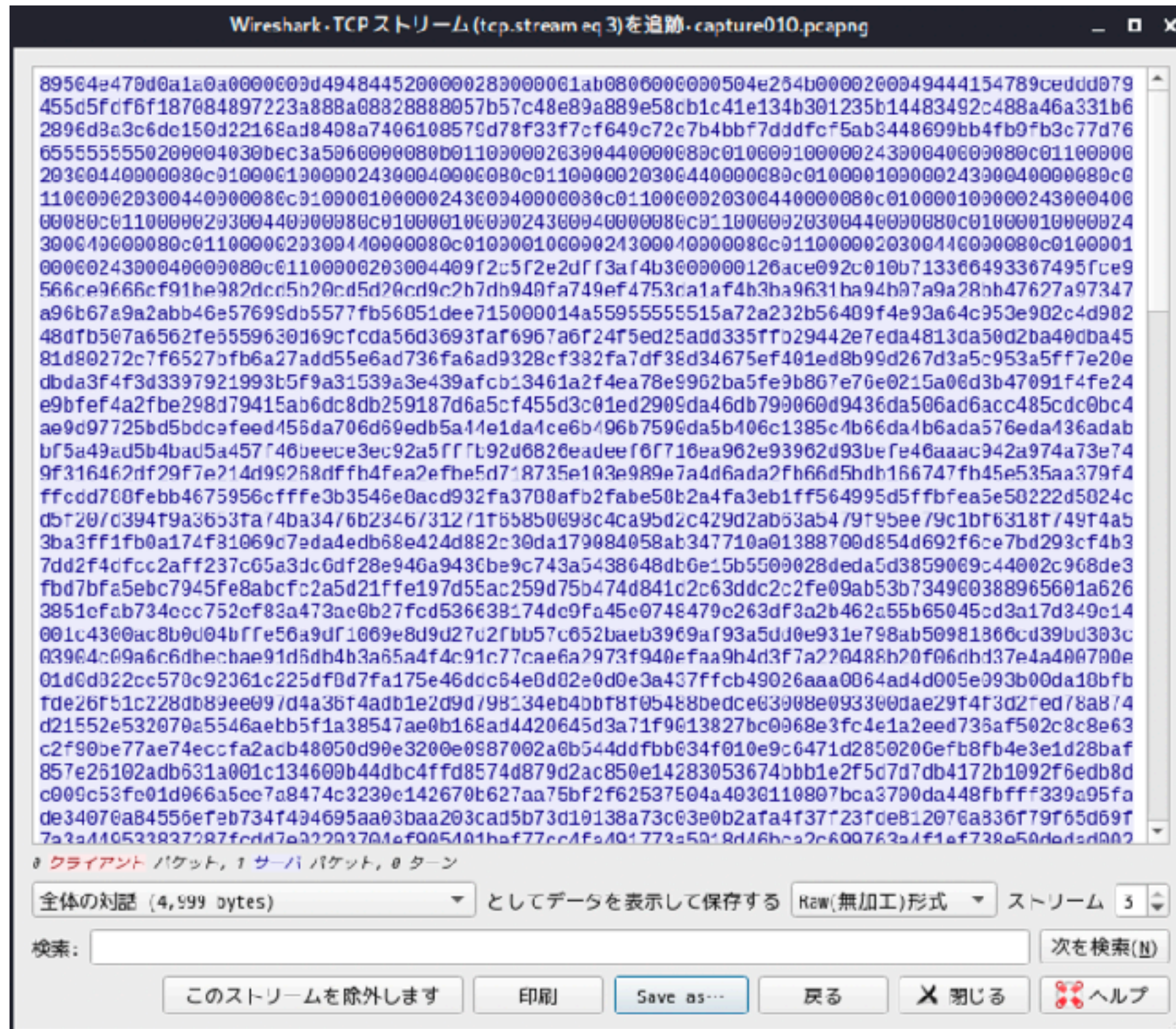
| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|---------------|---------------|-----------|--------|---|
| 102 | 10.557339696 | 192.168.10.14 | 192.168.10.12 | FTP-DA... | 5067 | FTP Data: 5001 bytes (PASV) (RETR /home/kali/MGT202105/xac) |
| 127 | 10.608226627 | 192.168.10.14 | 192.168.10.12 | FTP-DA... | 5065 | FTP Data: 4999 bytes (PASV) (RETR /home/kali/MGT202105/xab) |
| 150 | 10.634265449 | 192.168.10.14 | 192.168.10.12 | FTP-DA... | 5065 | FTP Data: 4999 bytes (PASV) (RETR /home/kali/MGT202105/xaa) |

Frame 102: 5067 bytes on wire (40536 bits), 5067 bytes captured (40536 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_4c:14:d6 (08:00:27:4c:14:d6), Dst: Apple_1f:f8:80 (8c:85:90:1f:f8:80)
Internet Protocol Version 4, Src: 192.168.10.14, Dst: 192.168.10.12
Transmission Control Protocol, Src Port: 37900, Dst Port: 57541, Seq: 1, Ack: 1, Len: 5001
FTP Data (5001 bytes data)
[\[Setup frame: 95\]](#)
[Setup method: PASV]
[Command: RETR /home/kali/MGT202105/xac]
[Command frame: 100](#)

0000 8c 85 90 1f f8 80 08 00 27 4c 14 d6 08 00 45 08 'L...E.
0010 13 bd 0d d1 40 00 40 06 83 f7 c0 a8 0a 0e c0 a8@..@.....
0020 0a 0c 94 0c e0 c5 e0 9d 59 6d b0 32 40 11 80 18 Ym.2@...
0030 01 fe a9 1a 00 00 01 01 08 0a 06 8b 00 37 27 2d7'-.
0040 d8 a2 f1 0f a0 a9 e1 4f d5 f7 9f dd b3 b3 8e 8f0.....
0050 df 12 68 c1 bf b1 0f 07 e5 56 c7 3b 80 49 20 f0 ..h.....V;.I..
0060 9f 55 1e 49 5a 3f ec a1 5b 4c c5 50 53 21 50 24 ..U·IZ?..[L·PS!P\$
0070 91 46 10 4a 9b 75 9d c5 6d b9 b2 f3 68 41 a4 31 ..F·J·u..m...hA·1
0080 f7 3d 9e ac d0 56 91 c7 19 e3 65 3f 63 01 35 ae ..=...V...e?c·5·
0090 62 1f 6e d6 52 11 e7 41 68 ad 2f bf 39 2f de 7e b·n·R·A h·/·9/·~
00a0 a9 f6 33 c3 4f 6a fc f7 db f1 5b eb d3 4b 37 4b ..3·0j...[·K7K

FTP Data: Protocol パケット数: 195 · 表示: 3 (1.5%) プロファイル: Default

xaaをダウンロードしたフレームのストリームを見ると、PNGファイルをダウンロードした事がわかる。よって、Save as...で出力する。
注意：バイナリデータの出力時はRaw形式で出力する。



xaaをファイルマネージャーや、ブラウザで見ると画像の一部が見える。画像の一部がxaaなのがあるので、xaaとxab,xacを繋げてみる。すると画像全体が復元される。ちなみに、xaa,xab,xac...というのは、splitコマンドでファイルを分割した際のデフォルトのファイル名



xaa

```
kali@kali:~/デスクトップ$ cat xa* > flag.png
```