ネットワーク関連
ユーティリティプログラム

千代浩司
高エネルギー加速器研究機構
素粒子原子核研究所

ネットワーク関連ユーティリティ

- nc (netcat)
- tcpdump
- wireshark

nc (netcat)

- nc - arbitrary TCP and UDP connections and listens
  - 標準入力をネットワークへ
  - ネットワークからのデータを標準出力へ

```
% nc   -l   1234
(これで待機して別の端末から)

Hello, worldと表示される
```

```
% nc   127.0.0.1   1234
Hello, worldと入力、エンターキー
```

- リードアウトモジュール 192.168.10.16、ポート24からTCPでデータがくるとして
  - nc 192.168.10.16 24 > datafile
  - nc 192.168.10.16 | prog_histo
  - nc 192.168.10.16 | tee datafile | prog_histo

ネットワークパケットキャプチャ

- ネットワークを流れるパケットをキャプチャするツール
  - コマンドライン: tcpdump
  - GUI 付き: wireshark
- 利用シーン
  - 接続できないんだけどパケットはでているのか？
  - データが読めないんだけど向こうからパケットはきているんでしょうか？
- (注意)
  - パケットキャプチャしているときにセンシティブな情報も見えることがあるので注意すること

tcpdump

- 単純な起動方法
  - sudo tcpdump　あるいは rootになってtcpdump
  - デフォルトのネットワークインターフェイスをダンプ
- ネットワークカードが複数あるのでどれかを指定する: -i eth1
  - tcpdump -i eth1
- IPアドレスで表示する: -n
  - tcpdump -n -i eth1
- ポート名も数字で表示する:
  - tcpdump -nn -i eth1
- キャプチャした内容をファイルに保存:
  - tcpdump -w file.cap

tcpdump

- キャプチャファイルを読む: -r file.cap
  - tcpdump -r file.cap
- 特定のパケットのみ読む:
  - and, or
  - host 192.168.10.16
  - port 80
  - src 192.168.10.16
  - dst 192.168.10.17
  - 例 : tcudump -r filecap src 192.168.10.16 and port 80
- 日付フォーマット
  - -t: 時刻情報を表示しない -tt: Epochからの経過秒を表示する

tcpdump出力例

TCPの3wayハンドシェイク付近:

11:27:55.137827 IP **192.168.0.16.59448 > 192.168.0.17.http:** S 153443204: 153443204(0) win 5840 <mss 1460,sackOK,timestamp 587094474 0,nop,wscale 7>
11:27:55.139573 IP **192.168.0.17.http > 192.168.0.16.59448**: S 4091282933: 4091282933(0) ack 153443205 win 65535 <mss 1460,nop,wscale 1,nop,nop,timestamp 3029380287 587094474,sackOK,eol>
11:27:55.139591 IP **192.168.0.16.59448 > 192.168.0.17.http**: . ack 1 win 46 <nop,nop,timestamp 587094479 3029380287>
11:27:55.139751 IP **192.168.0.16.59448 > 192.168.0.17.http**: P 1:103(102) ack 1 win 46 <nop,nop,timestamp 587094479 3029380287>
11:27:55.143520 IP **192.168.0.17.http > 192.168.0.16.59448**: P 1:252(251) ack103 win 33304 <nop,nop,timestamp 3029380290 587094479>

表示例: tcpdump -tt

```
1441158779.125073 IP 192.168.10.10.55056 > 192.168.10.20.80:
Flags [S], seq 3795629993, win 14600, options [mss
1460,nop,nop,sackOK,nop,wscale 9], length 0
1441158779.125545 IP 192.168.10.20.80 > 192.168.10.10.55056:
Flags [S.], seq 3897345900, ack 3795629994, win 14600, options
[mss 1460,nop,nop,sackOK,nop,wscale 6], length 0
1441158779.125574 IP 192.168.10.10.55056 > 192.168.10.20.80:
Flags [.], ack 1, win 29, length 0
1441158779.125716 IP 192.168.10.10.55056 > 192.168.10.20.80:
Flags [F.], seq 1, ack 1, win 29, length 0
1441158779.126098 IP 192.168.10.20.80 > 192.168.10.10.55056:
Flags [F.], seq 1, ack 2, win 229, length 0
1441158779.126113 IP 192.168.10.10.55056 > 192.168.10.20.80:
Flags [.], ack 2, win 29, length 0
```

tcpdump - 時刻情報

- 絶対時刻ではなくて相対的な時間に変換するプログラムを作っておくと便利なことがある。

0.000000 0.000000 IP **192.168.0.16.59448 > 192.168.0.17.http**: S 153443204:1534432
0.001746 0.001746 IP **192.168.0.17.http > 192.168.0.16.59448**: S 4091282933:409128
0.001764 0.000018 IP **192.168.0.16.59448 > 192.168.0.17.http**: . ack 1 win 46 <nop
0.001924 0.000160 IP **192.168.0.16.59448 > 192.168.0.17.http**: P 1:103(102) ack 1
0.005693 0.003769 IP **192.168.0.17.http > 192.168.0.16.59448**: P 1:252(251) ack 10
0.005703 0.000010 IP **192.168.0.16.59448 > 192.168.0.17.http**: . ack 252 win 54 <n
1.107822 1.102119 IP **192.168.0.16.59448 > 192.168.0.17.http**: F 103:103(0) ack 25
1.108482 0.000660 IP **192.168.0.17.http > 192.168.0.16.59448**: . ack 104 win 33304
1.109608 0.001126 IP **192.168.0.17.http > 192.168.0.16.59448**: F 252:252(0) ack 10
1.109618 0.000010 IP **192.168.0.16.59448 > 192.168.0.17.http**: . ack 253 win 54 <n

最初の欄はSYNを送ってからの経過時間
2番目の欄は直前の行との時間差を示すもの

tcpdump + program log

- tcpdumpの時刻情報と同じ時刻フォーマットでログを出すようにしておいてtcpdumpをとりつつプログラムを走らせあとからマージする:

  (tcpdump -n -r tcpdump.out; cat log) | sort -n

パケットの流れを見てみる

```
0.000000   0.000000   connect start (プログラムの出力)
0.000363   0.000363   IP 192.168.0.100.35005 > 192.168.0.101.13: S
0.000489   0.000126   IP 192.168.0.101.13      > 192.168.0.100.35005: S
0.000536   0.000047   IP 192.168.0.100.35005 > 192.168.0.101.13: . ack 1 win 1460
0.000583   0.000047   connect returns (プログラムの出力)

0.004302   0.003719   IP 192.168.0.101.13      > 192.168.0.100.35005: FP 1:27(26) ack 1
0.004718   0.000416   IP 192.168.0.100.35005 > 192.168.0.101.13: F 1:1(0) ack 28
0.004917   0.000199   IP 192.168.0.101.13      > 192.168.0.100.35005: . ack 2 win 33303
```

tcpdump: データパートも見る

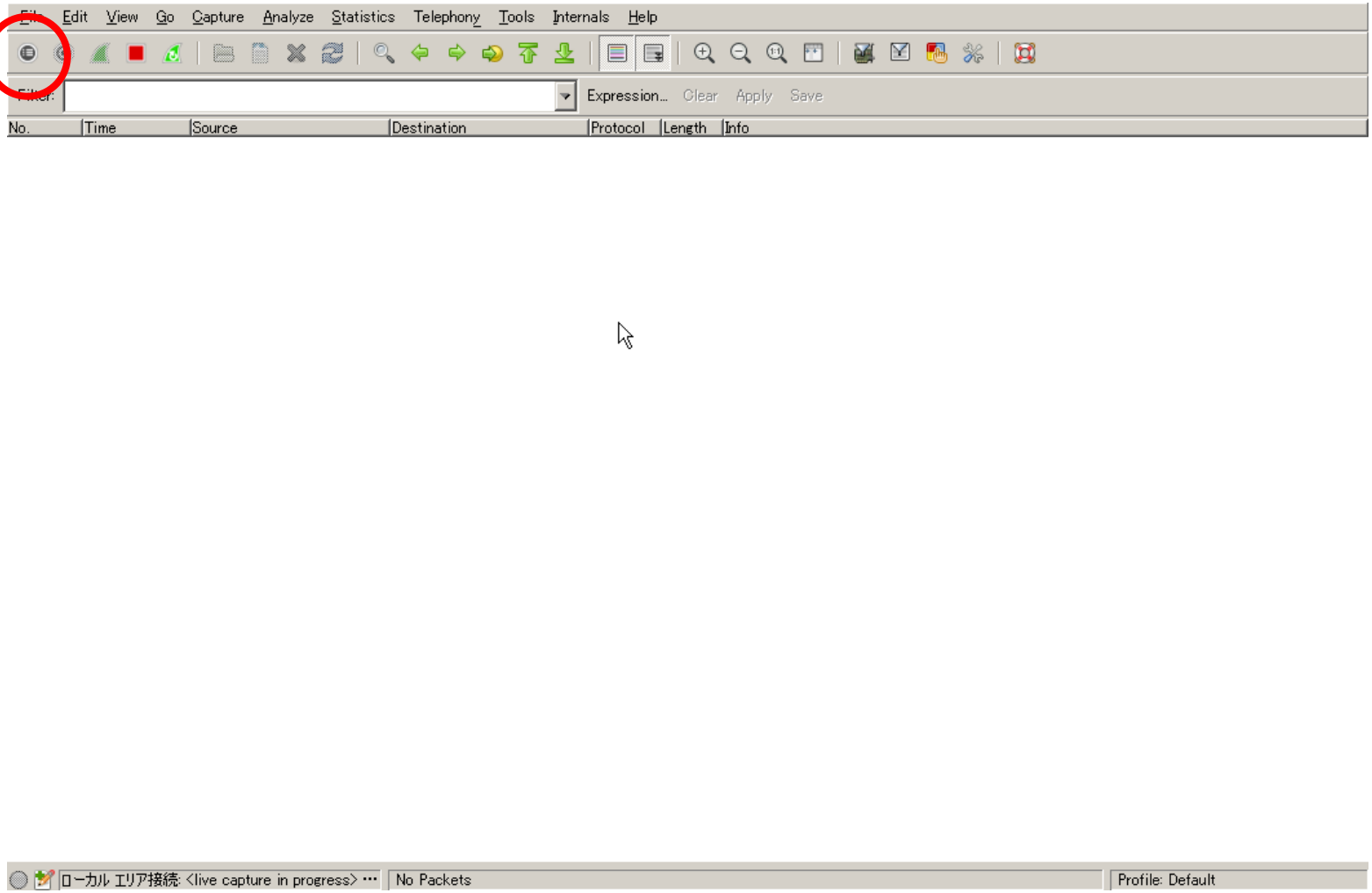
- tcpdump -X

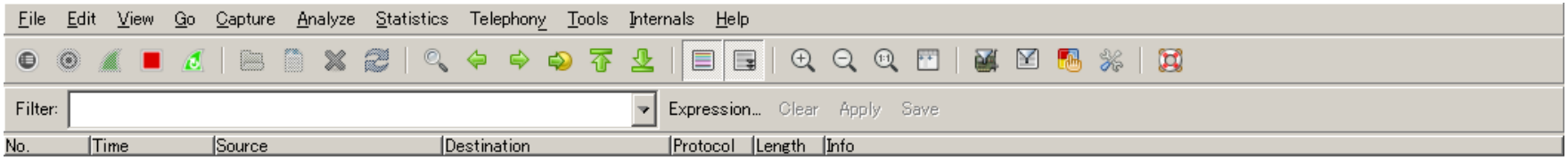
```
08:18:36.466963 IP 192.168.10.20.54155 > 192.168.10.102.2222: Flags [S], seq 2837954085, win 14600, options [mss 1460,nop,
nop,sackOK,nop,wscale 9], length 0
    0x0000:  4500 0034 95a5 4000 4006 0f54 c0a8 0a14  E..4..@.@..T....
    0x0010:  c0a8 0a66 d38b 08ae a927 be25 0000 0000  ...f.....'.%....
    0x0020:  8002 3908 5cb5 0000 0204 05b4 0101 0402  ..9.\...........
    0x0030:  0103 0309                                ....
08:18:36.467177 IP 192.168.10.102.2222 > 192.168.10.20.54155: Flags [S.], seq 3687851392, ack 2837954086, win 14600, optio
ns [mss 1460,nop,nop,sackOK,nop,wscale 7], length 0
    0x0000:  4500 0034 0000 4000 4006 a4f9 c0a8 0a66  E..4..@.@......f
    0x0010:  c0a8 0a14 08ae d38b dbd0 2580 a927 be26  ..........%..'.&
    0x0020:  8012 3908 5b55 0000 0204 05b4 0101 0402  ..9.[U..........
    0x0030:  0103 0307                                ....
08:18:36.467205 IP 192.168.10.20.54155 > 192.168.10.102.2222: Flags [.], ack 1, win 29, length 0
    0x0000:  4500 0028 95a6 4000 4006 0f5f c0a8 0a14  E..(..@.@.._....
    0x0010:  c0a8 0a66 d38b 08ae a927 be26 dbd0 2581  ...f.....'.&..%.
    0x0020:  5010 001d d512 0000                      P.......
08:18:36.467636 IP 192.168.10.102.2222 > 192.168.10.20.54155: Flags [P.], seq 1:1025, ack 1, win 115, length 1024
    0x0000:  4500 0428 6be4 4000 4006 3521 c0a8 0a66  E..(k.@.@.5!...f
    0x0010:  c0a8 0a14 08ae d38b dbd0 2581 a927 be26  ..........%..'.&
    0x0020:  5018 0073 d0b4 0000 0000 0000 0000 0000  P..s............
    0x0030:  0000 0000 0000 0000 0000 0000 0000 0000  ................
    0x0040:  0000 0000 0000 0000 0000 0000 0000 0000  ................
    0x0050:  0000 0000 0000 0000 0000 0000 0000 0000  ................
    0x0060:  0000 0000 0000 0000 0000 0000 0000 0000  ................
```

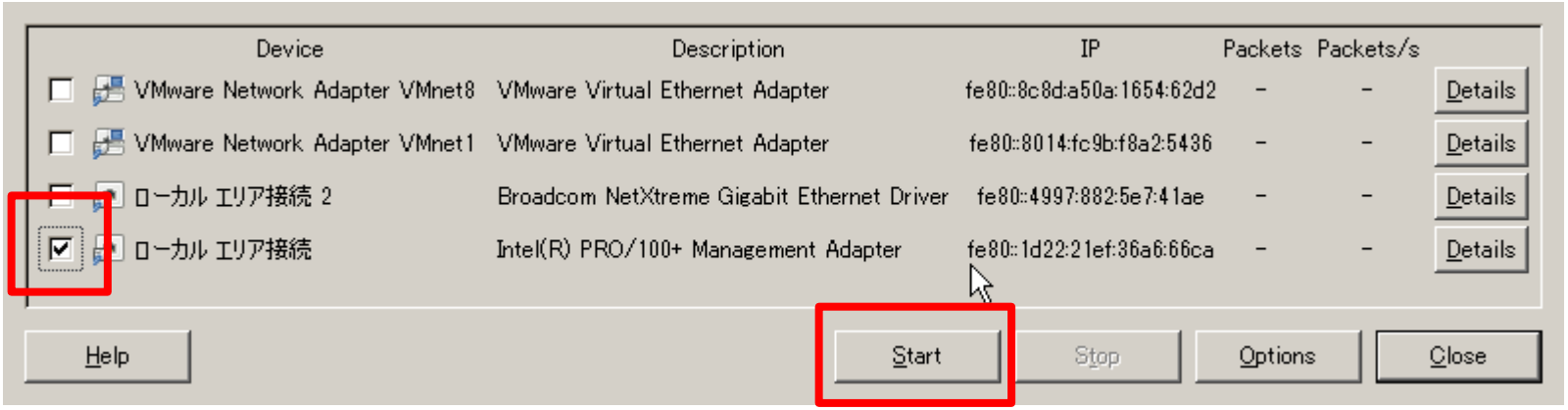
wireshark

- yum install wireshark-gnome (GUIつきのをインストールする）
- Windows版もある
- Ethernet、IP, TCPのヘッダがどこか色つきで表示してくれるので便利
- 単体で起動: wireshark
- すでにtcpdumpでキャプチャしたファイルを読む: wireshark -r file.cap

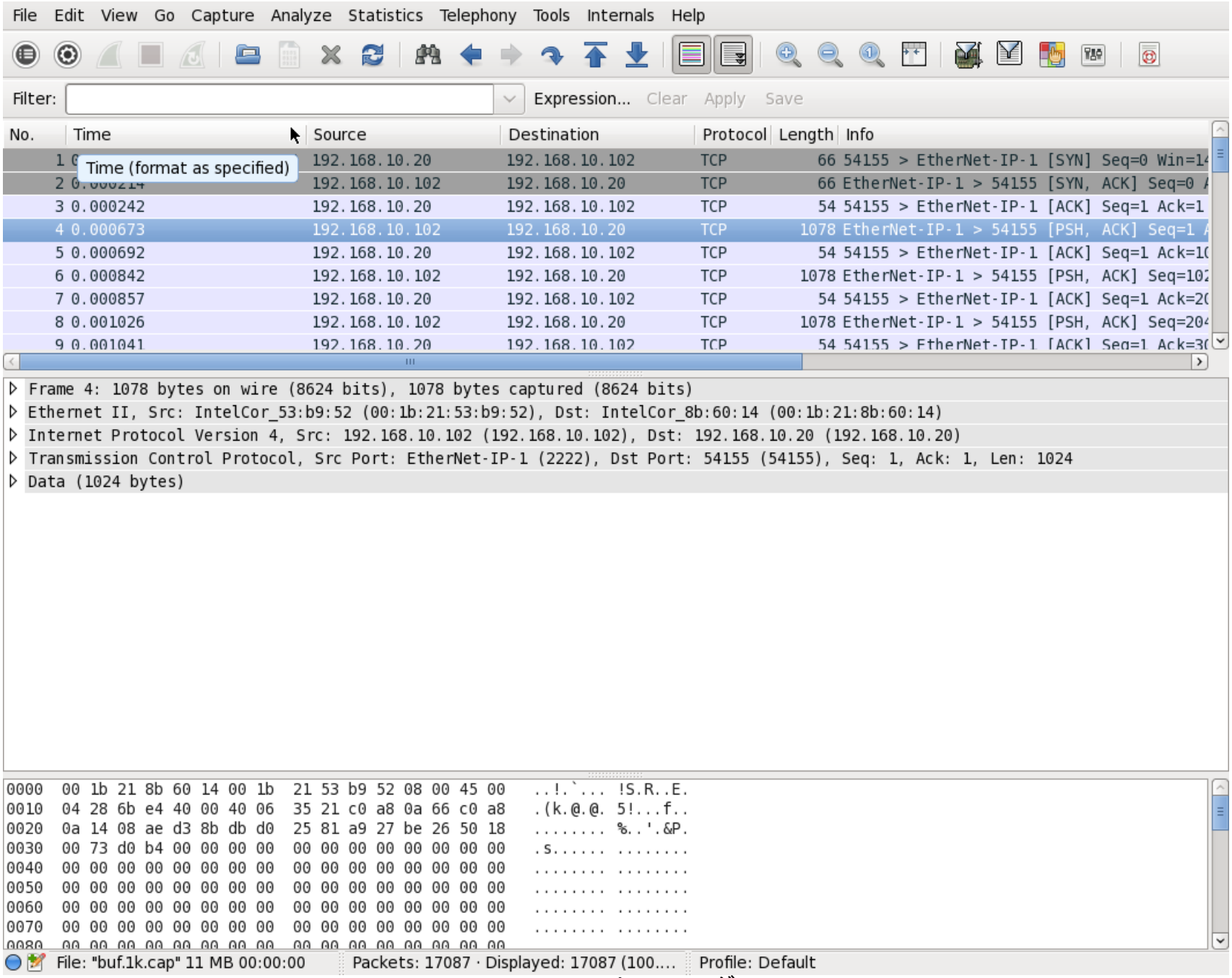
wireshark (Windows)

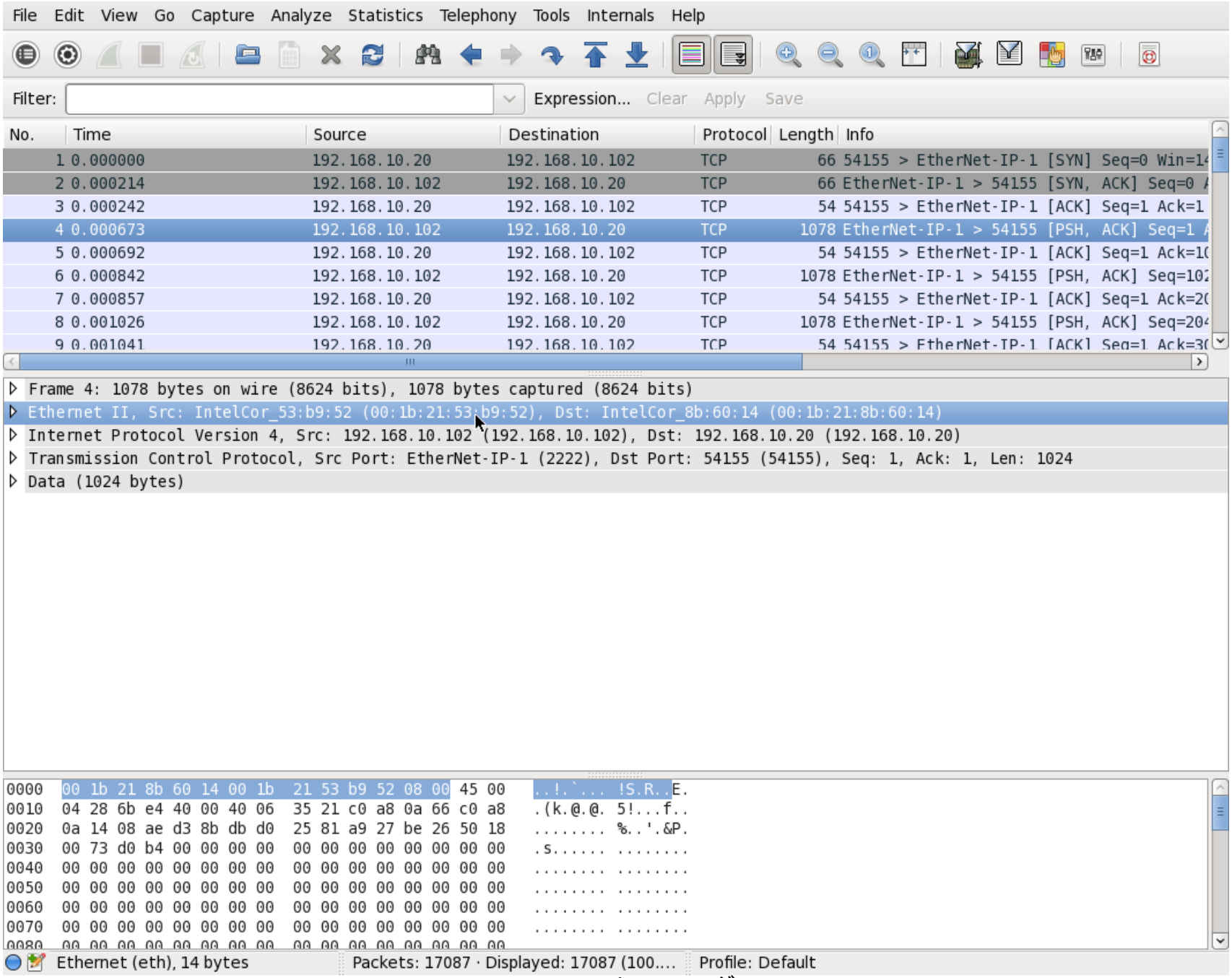


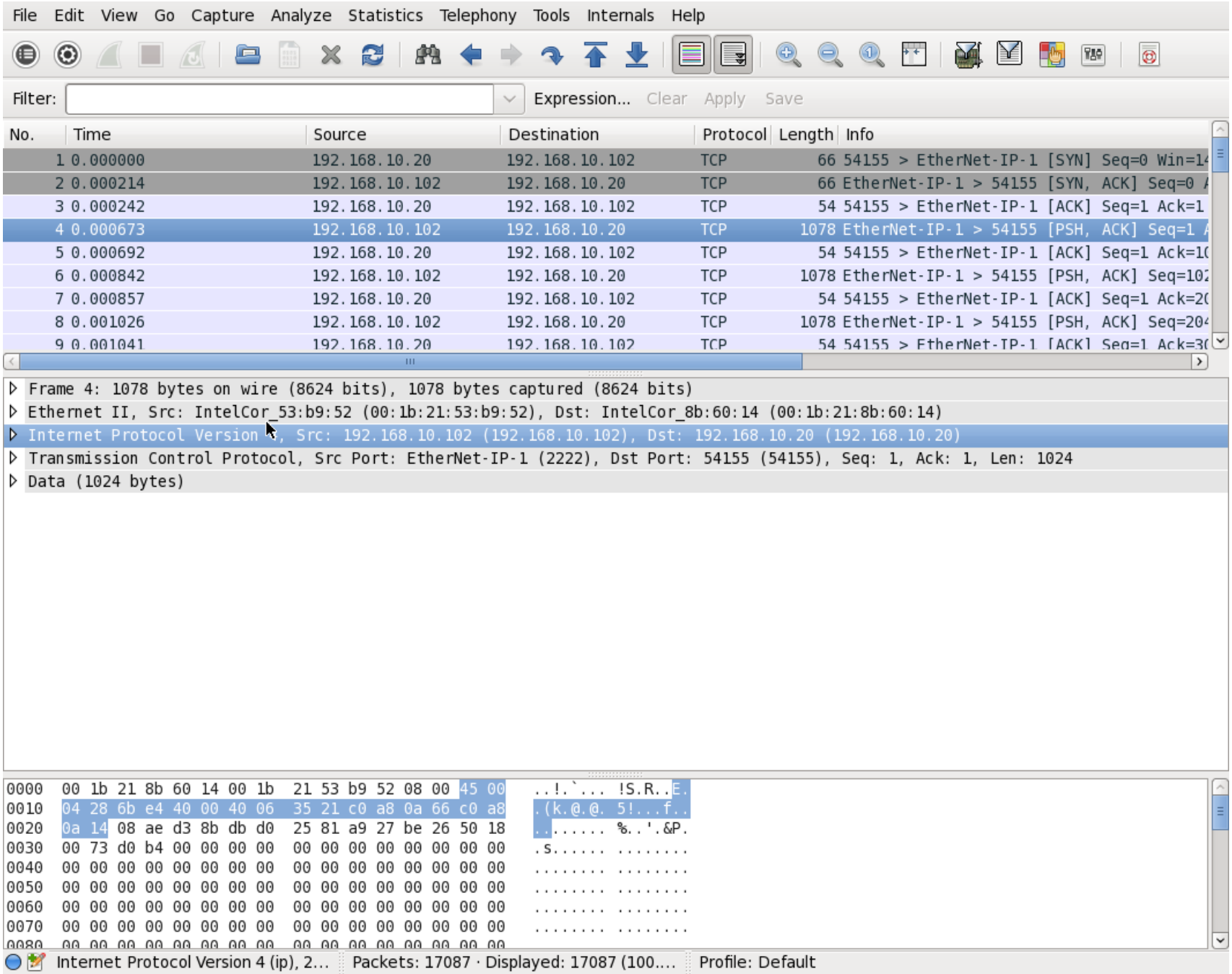

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info

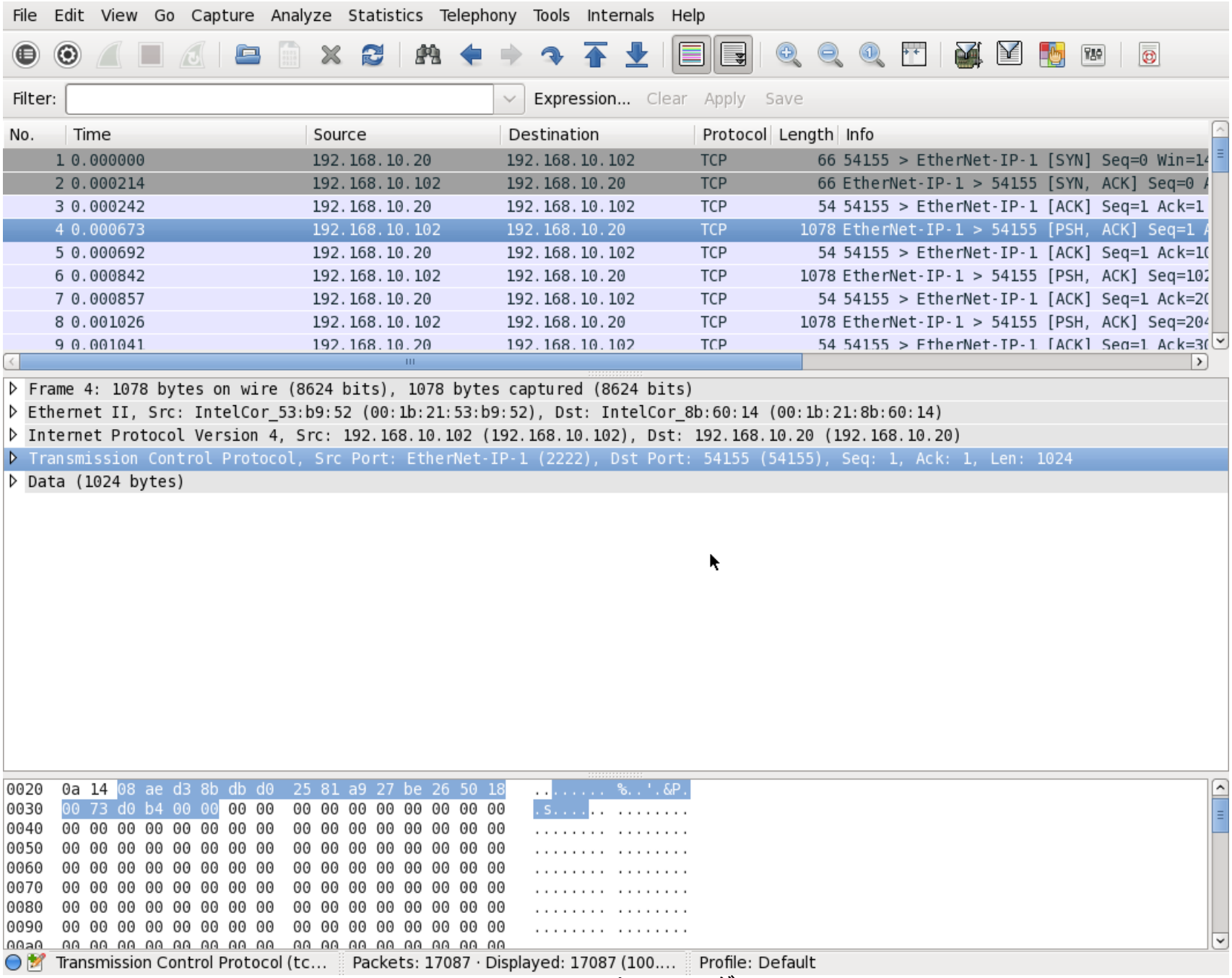

Device Description IP Packets Packets/s
VMware Network Adapter VMnet8 VMware Virtual Ethernet Adapter fe80::8c8d:a50a:1654:62d2 - - Details
VMware Network Adapter VMnet1 VMware Virtual Ethernet Adapter fe80::8014:fc9b:f8a2:5436 - - Details
ローカル エリア接続 2 Broadcom NetXtreme Gigabit Ethernet Driver fe80::4997:882:5e7:41ae - - Details
ローカル エリア接続 Intel(R) PRO/100+ Management Adapter fe80::1d22:21ef:36a6:66ca - - Details
Help
Start
Stop
Options
Close

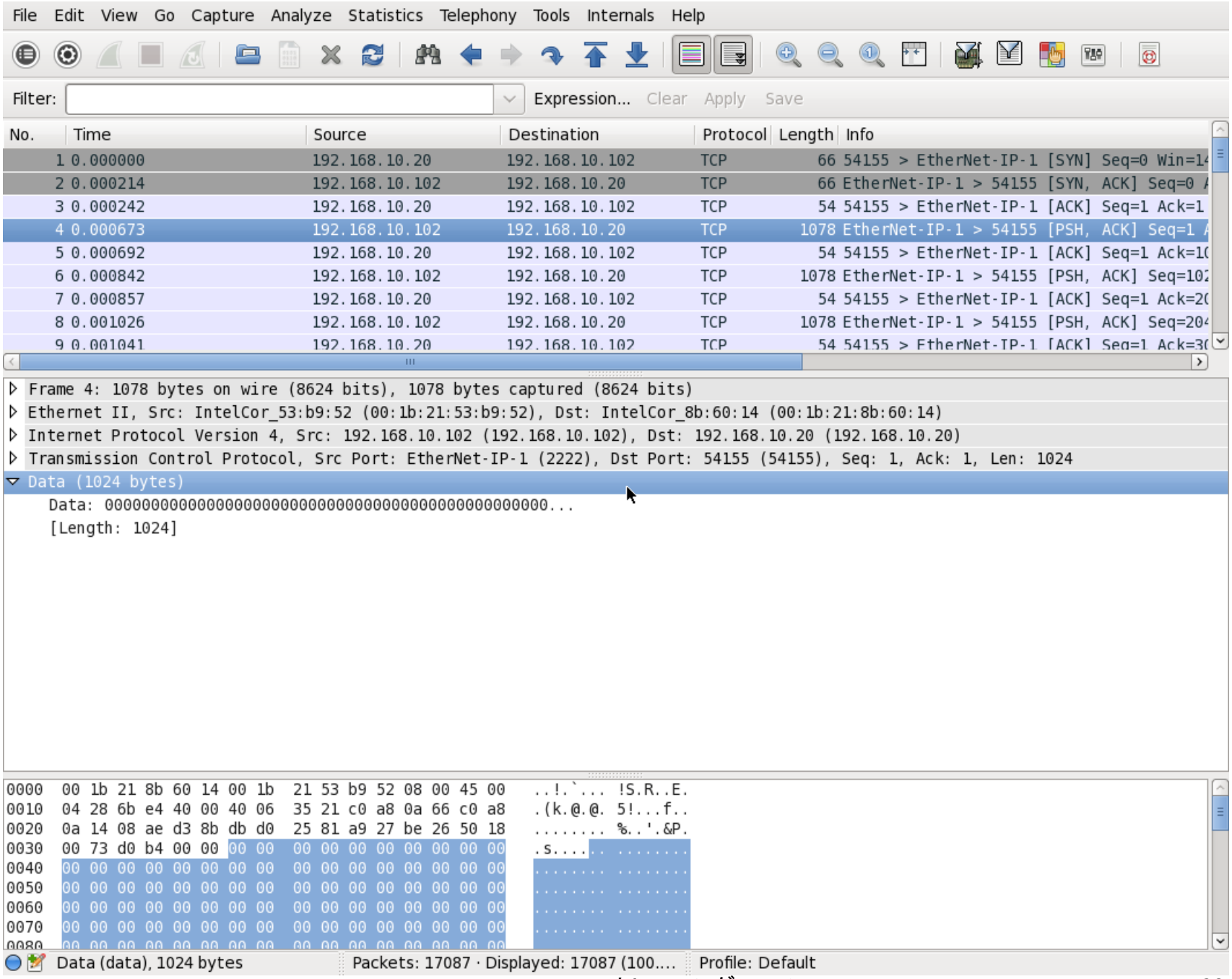

ローカル エリア接続: <live capture in progress>
No Packets
Profile: Default

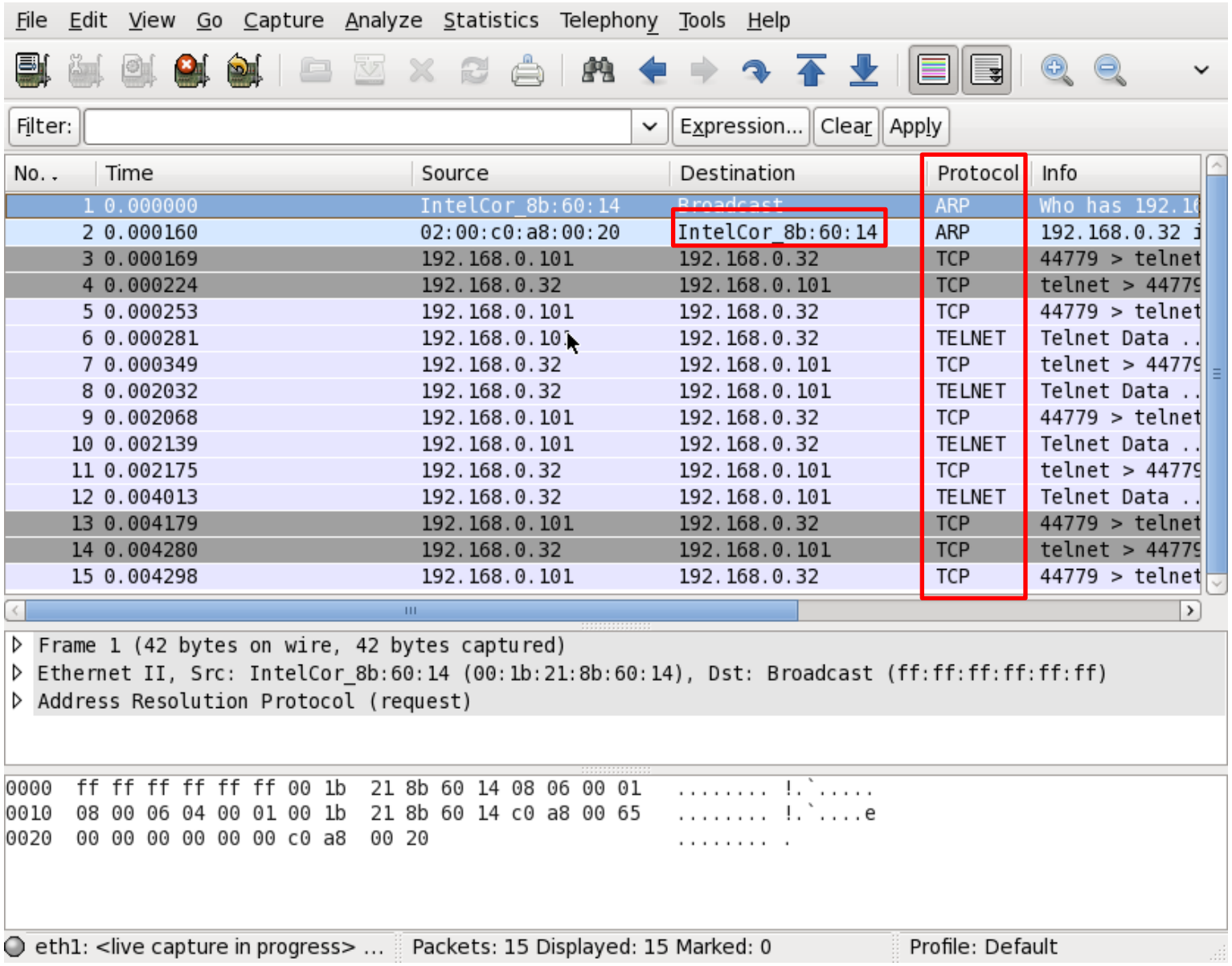

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
Time (format as specified)
1 0 192.168.10.20 192.168.10.102 TCP 66 54155 > EtherNet-IP-1 [SYN] Seq=0 Win=14
2 0.000214 192.168.10.102 192.168.10.20 TCP 66 EtherNet-IP-1 > 54155 [SYN, ACK] Seq=0 A
3 0.000242 192.168.10.20 192.168.10.102 TCP 54 54155 > EtherNet-IP-1 [ACK] Seq=1 Ack=1
4 0.000673 192.168.10.102 192.168.10.20 TCP 1078 EtherNet-IP-1 > 54155 [PSH, ACK] Seq=1 A
5 0.000692 192.168.10.20 192.168.10.102 TCP 54 54155 > EtherNet-IP-1 [ACK] Seq=1 Ack=10
6 0.000842 192.168.10.102 192.168.10.20 TCP 1078 EtherNet-IP-1 > 54155 [PSH, ACK] Seq=102
7 0.000857 192.168.10.20 192.168.10.102 TCP 54 54155 > EtherNet-IP-1 [ACK] Seq=1 Ack=20
8 0.001026 192.168.10.102 192.168.10.20 TCP 1078 EtherNet-IP-1 > 54155 [PSH, ACK] Seq=204
9 0.001041 192.168.10.20 192.168.10.102 TCP 54 54155 > EtherNet-IP-1 [ACK] Seq=1 Ack=30
Frame 4: 1078 bytes on wire (8624 bits), 1078 bytes captured (8624 bits)
Ethernet II, Src: IntelCor_53:b9:52 (00:1b:21:53:b9:52), Dst: IntelCor_8b:60:14 (00:1b:21:8b:60:14)
Internet Protocol Version 4, Src: 192.168.10.102 (192.168.10.102), Dst: 192.168.10.20 (192.168.10.20)
Transmission Control Protocol, Src Port: EtherNet-IP-1 (2222), Dst Port: 54155 (54155), Seq: 1, Ack: 1, Len: 1024
Data (1024 bytes)
0000 00 1b 21 8b 60 14 00 1b 21 53 b9 52 08 00 45 00 ..!.`... !S.R..E.
0010 04 28 6b e4 40 00 40 06 35 21 c0 a8 0a 66 c0 a8 .(k.@.@. 5!...f..
0020 0a 14 08 ae d3 8b db d0 25 81 a9 27 be 26 50 18 .... %..'.&P.
0030 00 73 d0 b4 00 00 00 00 00 00 00 00 00 00 00 00 .s...... ....
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
File: "buf.1k.cap" 11 MB 00:00:00 Packets: 17087 · Displayed: 17087 (100.... Profile: Default


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.10.20 192.168.10.102 TCP 66 54155 > EtherNet-IP-1 [SYN] Seq=0 Win=14
2 0.000214 192.168.10.102 192.168.10.20 TCP 66 EtherNet-IP-1 > 54155 [SYN, ACK] Seq=0 A
3 0.000242 192.168.10.20 192.168.10.102 TCP 54 54155 > EtherNet-IP-1 [ACK] Seq=1 Ack=1
4 0.000673 192.168.10.102 192.168.10.20 TCP 1078 EtherNet-IP-1 > 54155 [PSH, ACK] Seq=1 A
5 0.000692 192.168.10.20 192.168.10.102 TCP 54 54155 > EtherNet-IP-1 [ACK] Seq=1 Ack=1(
6 0.000842 192.168.10.102 192.168.10.20 TCP 1078 EtherNet-IP-1 > 54155 [PSH, ACK] Seq=10
7 0.000857 192.168.10.20 192.168.10.102 TCP 54 54155 > EtherNet-IP-1 [ACK] Seq=1 Ack=2(
8 0.001026 192.168.10.102 192.168.10.20 TCP 1078 EtherNet-IP-1 > 54155 [PSH, ACK] Seq=20
9 0.001041 192.168.10.20 192.168.10.102 TCP 54 54155 > EtherNet-IP-1 [ACK] Seq=1 Ack=3(
Frame 4: 1078 bytes on wire (8624 bits), 1078 bytes captured (8624 bits)
Ethernet II, Src: IntelCor_53:b9:52 (00:1b:21:53:b9:52), Dst: IntelCor_8b:60:14 (00:1b:21:8b:60:14)
Internet Protocol Version 4, Src: 192.168.10.102 (192.168.10.102), Dst: 192.168.10.20 (192.168.10.20)
Transmission Control Protocol, Src Port: EtherNet-IP-1 (2222), Dst Port: 54155 (54155), Seq: 1, Ack: 1, Len: 1024
Data (1024 bytes)
0000 00 1b 21 8b 60 14 00 1b 21 53 b9 52 08 00 45 00 ..!.`... !S.R..E.
0010 04 28 6b e4 40 00 40 06 35 21 c0 a8 0a 66 c0 a8 .(k.@.@. 5!...f..
0020 0a 14 08 ae d3 8b db d0 25 81 a9 27 be 26 50 18 .... %..'.&P.
0030 00 73 d0 b4 00 00 00 00 00 00 00 00 00 00 00 00 .s...... ....
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
Ethernet (eth), 14 bytes
Packets: 17087 · Displayed: 17087 (100....
Profile: Default

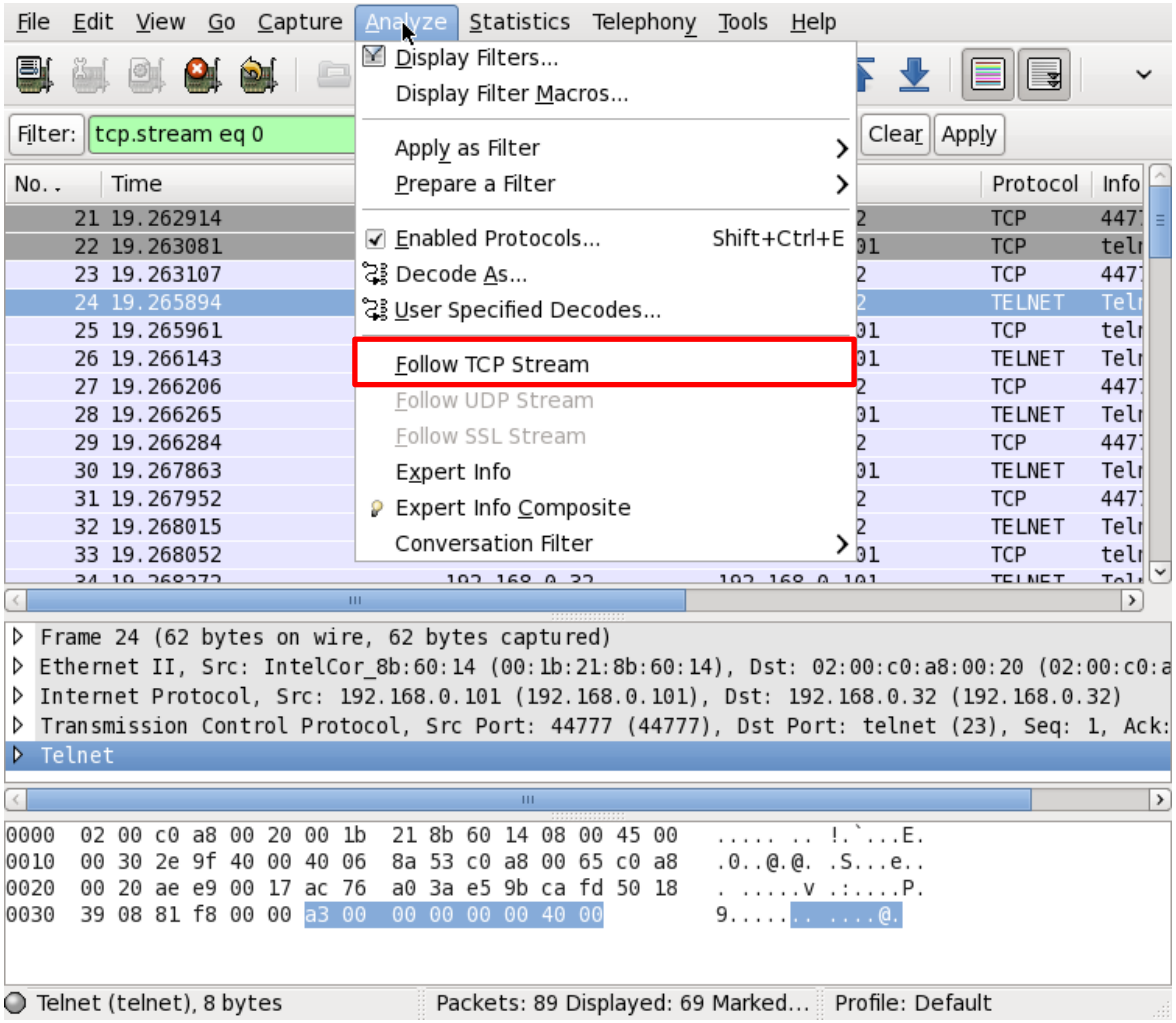

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.10.20 192.168.10.102 TCP 66 54155 > EtherNet-IP-1 [SYN] Seq=0 Win=14
2 0.000214 192.168.10.102 192.168.10.20 TCP 66 EtherNet-IP-1 > 54155 [SYN, ACK] Seq=0 A
3 0.000242 192.168.10.20 192.168.10.102 TCP 54 54155 > EtherNet-IP-1 [ACK] Seq=1 Ack=1
4 0.000673 192.168.10.102 192.168.10.20 TCP 1078 EtherNet-IP-1 > 54155 [PSH, ACK] Seq=1 A
5 0.000692 192.168.10.20 192.168.10.102 TCP 54 54155 > EtherNet-IP-1 [ACK] Seq=1 Ack=1(
6 0.000842 192.168.10.102 192.168.10.20 TCP 1078 EtherNet-IP-1 > 54155 [PSH, ACK] Seq=10
7 0.000857 192.168.10.20 192.168.10.102 TCP 54 54155 > EtherNet-IP-1 [ACK] Seq=1 Ack=2(
8 0.001026 192.168.10.102 192.168.10.20 TCP 1078 EtherNet-IP-1 > 54155 [PSH, ACK] Seq=20
9 0.001041 192.168.10.20 192.168.10.102 TCP 54 54155 > EtherNet-IP-1 [ACK] Seq=1 Ack=3(
Frame 4: 1078 bytes on wire (8624 bits), 1078 bytes captured (8624 bits)
Ethernet II, Src: IntelCor_53:b9:52 (00:1b:21:53:b9:52), Dst: IntelCor_8b:60:14 (00:1b:21:8b:60:14)
Internet Protocol Version 4, Src: 192.168.10.102 (192.168.10.102), Dst: 192.168.10.20 (192.168.10.20)
Transmission Control Protocol, Src Port: EtherNet-IP-1 (2222), Dst Port: 54155 (54155), Seq: 1, Ack: 1, Len: 1024
Data (1024 bytes)
0000 00 1b 21 8b 60 14 00 1b 21 53 b9 52 08 00 45 00 ..!.`... !S.R..E.
0010 04 28 6b e4 40 00 40 06 35 21 c0 a8 0a 66 c0 a8 .(k.@.@. 5!...f..
0020 0a 14 08 ae d3 8b db d0 25 81 a9 27 be 26 50 18 .... %..'.&P.
0030 00 73 d0 b4 00 00 00 00 00 00 00 00 00 00 00 00 .s...... ....
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
Internet Protocol Version 4 (ip), 2...
Packets: 17087 · Displayed: 17087 (100....
Profile: Default


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.10.20 192.168.10.102 TCP 66 54155 > EtherNet-IP-1 [SYN] Seq=0 Win=14
2 0.000214 192.168.10.102 192.168.10.20 TCP 66 EtherNet-IP-1 > 54155 [SYN, ACK] Seq=0 A
3 0.000242 192.168.10.20 192.168.10.102 TCP 54 54155 > EtherNet-IP-1 [ACK] Seq=1 Ack=1
4 0.000673 192.168.10.102 192.168.10.20 TCP 1078 EtherNet-IP-1 > 54155 [PSH, ACK] Seq=1 A
5 0.000692 192.168.10.20 192.168.10.102 TCP 54 54155 > EtherNet-IP-1 [ACK] Seq=1 Ack=1(
6 0.000842 192.168.10.102 192.168.10.20 TCP 1078 EtherNet-IP-1 > 54155 [PSH, ACK] Seq=10
7 0.000857 192.168.10.20 192.168.10.102 TCP 54 54155 > EtherNet-IP-1 [ACK] Seq=1 Ack=2(
8 0.001026 192.168.10.102 192.168.10.20 TCP 1078 EtherNet-IP-1 > 54155 [PSH, ACK] Seq=20
9 0.001041 192.168.10.20 192.168.10.102 TCP 54 54155 > EtherNet-IP-1 [ACK] Seq=1 Ack=3(
Frame 4: 1078 bytes on wire (8624 bits), 1078 bytes captured (8624 bits)
Ethernet II, Src: IntelCor_53:b9:52 (00:1b:21:53:b9:52), Dst: IntelCor_8b:60:14 (00:1b:21:8b:60:14)
Internet Protocol Version 4, Src: 192.168.10.102 (192.168.10.102), Dst: 192.168.10.20 (192.168.10.20)
Transmission Control Protocol, Src Port: EtherNet-IP-1 (2222), Dst Port: 54155 (54155), Seq: 1, Ack: 1, Len: 1024
Data (1024 bytes)
0020 0a 14 08 ae d3 8b db d0 25 81 a9 27 be 26 50 18 ..... %..'.&P.
0030 00 73 d0 b4 00 00 00 00 00 00 00 00 00 00 00 00 .s..... ....
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
Transmission Control Protocol (tc... Packets: 17087 · Displayed: 17087 (100.... Profile: Default


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.10.20 192.168.10.102 TCP 66 54155 > EtherNet-IP-1 [SYN] Seq=0 Win=14
2 0.000214 192.168.10.102 192.168.10.20 TCP 66 EtherNet-IP-1 > 54155 [SYN, ACK] Seq=0 A
3 0.000242 192.168.10.20 192.168.10.102 TCP 54 54155 > EtherNet-IP-1 [ACK] Seq=1 Ack=1
4 0.000673 192.168.10.102 192.168.10.20 TCP 1078 EtherNet-IP-1 > 54155 [PSH, ACK] Seq=1 A
5 0.000692 192.168.10.20 192.168.10.102 TCP 54 54155 > EtherNet-IP-1 [ACK] Seq=1 Ack=1(
6 0.000842 192.168.10.102 192.168.10.20 TCP 1078 EtherNet-IP-1 > 54155 [PSH, ACK] Seq=10
7 0.000857 192.168.10.20 192.168.10.102 TCP 54 54155 > EtherNet-IP-1 [ACK] Seq=1 Ack=2(
8 0.001026 192.168.10.102 192.168.10.20 TCP 1078 EtherNet-IP-1 > 54155 [PSH, ACK] Seq=20
9 0.001041 192.168.10.20 192.168.10.102 TCP 54 54155 > EtherNet-IP-1 [ACK] Seq=1 Ack=3(
Frame 4: 1078 bytes on wire (8624 bits), 1078 bytes captured (8624 bits)
Ethernet II, Src: IntelCor_53:b9:52 (00:1b:21:53:b9:52), Dst: IntelCor_8b:60:14 (00:1b:21:8b:60:14)
Internet Protocol Version 4, Src: 192.168.10.102 (192.168.10.102), Dst: 192.168.10.20 (192.168.10.20)
Transmission Control Protocol, Src Port: EtherNet-IP-1 (2222), Dst Port: 54155 (54155), Seq: 1, Ack: 1, Len: 1024
Data (1024 bytes)
Data: 0000000000000000000000000000000000000000000000000000...
[Length: 1024]
0000 00 1b 21 8b 60 14 00 1b 21 53 b9 52 08 00 45 00 ..!.`... !S.R..E.
0010 04 28 6b e4 40 00 40 06 35 21 c0 a8 0a 66 c0 a8 .(k.@.@. 5!...f..
0020 0a 14 08 ae d3 8b db d0 25 81 a9 27 be 26 50 18 .... %..'.&P.
0030 00 73 d0 b4 00 00 00 00 00 00 00 00 00 00 00 00 .s...... ....
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
Data (data), 1024 bytes
Packets: 17087 · Displayed: 17087 (100....
Profile: Default



MACアドレスからベンダーを調べて表示する（らしい）



- キャプチャファイルに複数のTCPセッションがあってもAnalyze→Follow TCP Streamで追跡可能

TCPで再送が起きた場合の例