

# 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 packets のみ読む:
  - and, or
  - host 192.168.10.16
  - port 80
  - src 192.168.10.16
  - dst 192.168.10.17
  - 例: tcpdump -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おことがある。

```
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
```

# パケットの流れをしてみる

```
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

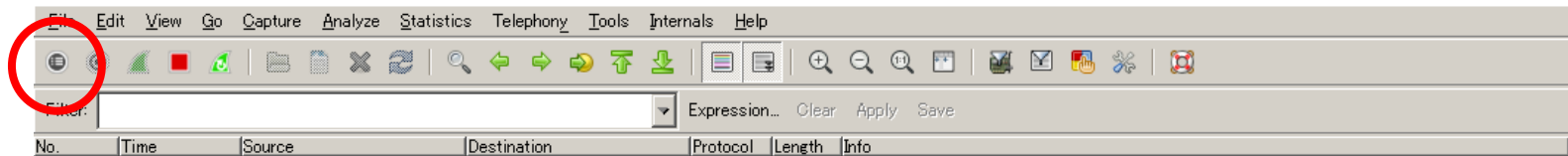
- tcpdump -X

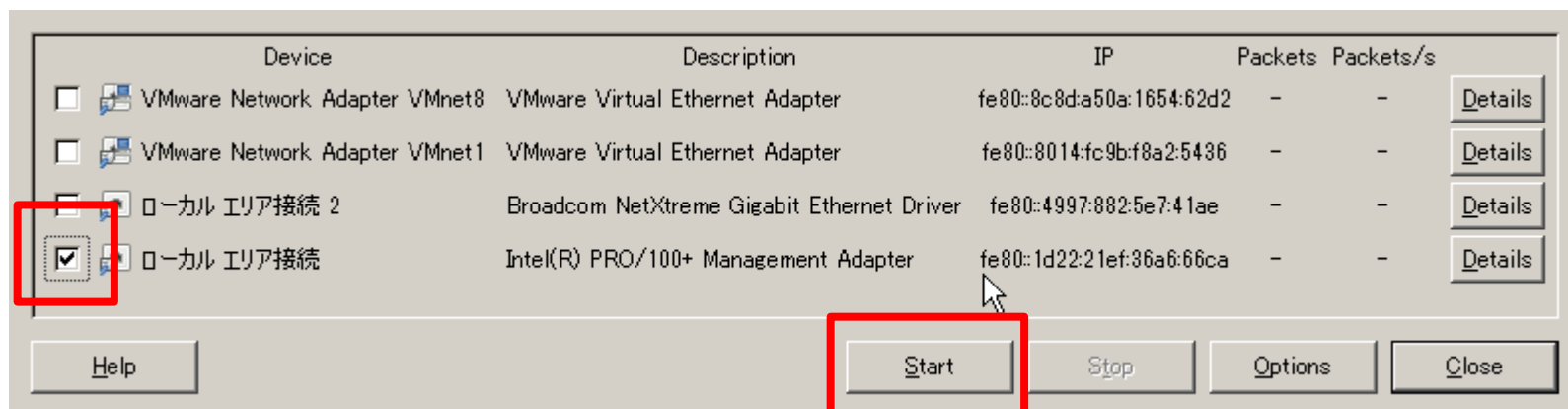
```
08:18:36.466963 IP 192.168.10.20.54155 > 192.168.10.102.2222: Flags [S], seq 2837954085, win 14600, options [mss 1460,nop,
nop,sackOK,nop,wscale 9], length 0
 0x0000: 4500 0034 95a5 4000 4006 0f54 c0a8 0a14 E..4..@.@..T....
 0x0010: c0a8 0a66 d38b 08ae a927 be25 0000 0000 ...f.....'%.%....
 0x0020: 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)







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
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
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=10
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=20
9	0.001041	192.168.10.20	192.168.10.102	TCP	54	54155 > EtherNet-IP-1 [ACK] Seq=1 Ack=30

Time (format as specified)

▶ 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  .....
0080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
  
```





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
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
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=10
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=20
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  .....
0080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
  
```



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
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
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=10
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=20
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  .S.....
0040  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  .....
0060  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  .....
0080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
  
```



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
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
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=10
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=20
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)

```

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  .s . . . . .
0040  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  .....
0060  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  .....
0080  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  .....
00a0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
  
```



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
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
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=10
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=20
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)  
 Data: 00...  
 [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	.s....
0040	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	.....
0060	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	.....
0080	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

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No. .	Time	Source	Destination	Protocol	Info
1	0.000000	IntelCor_8b:60:14	Broadcast	ARP	Who has 192.168.0.32
2	0.000160	02:00:c0:a8:00:20	IntelCor_8b:60:14	ARP	192.168.0.32 j
3	0.000169	192.168.0.101	192.168.0.32	TCP	44779 > telnet
4	0.000224	192.168.0.32	192.168.0.101	TCP	telnet > 44779
5	0.000253	192.168.0.101	192.168.0.32	TCP	44779 > telnet
6	0.000281	192.168.0.101	192.168.0.32	TELNET	Telnet Data ..
7	0.000349	192.168.0.32	192.168.0.101	TCP	telnet > 44779
8	0.002032	192.168.0.32	192.168.0.101	TELNET	Telnet Data ..
9	0.002068	192.168.0.101	192.168.0.32	TCP	44779 > telnet
10	0.002139	192.168.0.101	192.168.0.32	TELNET	Telnet Data ..
11	0.002175	192.168.0.32	192.168.0.101	TCP	telnet > 44779
12	0.004013	192.168.0.32	192.168.0.101	TELNET	Telnet Data ..
13	0.004179	192.168.0.101	192.168.0.32	TCP	44779 > telnet
14	0.004280	192.168.0.32	192.168.0.101	TCP	telnet > 44779
15	0.004298	192.168.0.101	192.168.0.32	TCP	44779 > telnet

Frame 1 (42 bytes on wire, 42 bytes captured)

Ethernet II, Src: IntelCor\_8b:60:14 (00:1b:21:8b:60:14), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Address Resolution Protocol (request)

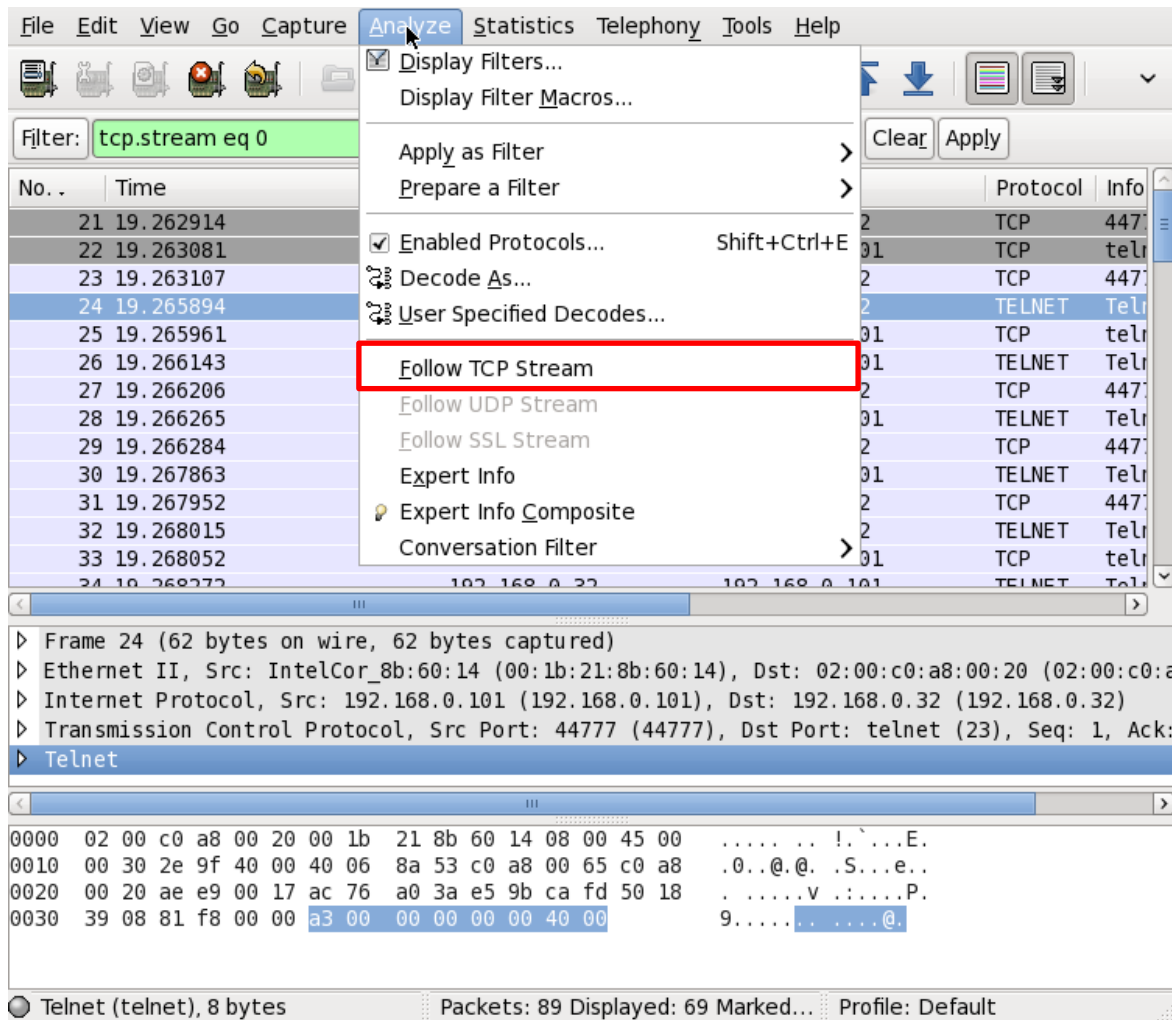
```

0000  ff ff ff ff ff ff 00 1b 21 8b 60 14 08 06 00 01  ..... !\.....
0010  08 00 06 04 00 01 00 1b 21 8b 60 14 c0 a8 00 65  ..... !\.....e
0020  00 00 00 00 00 00 c0 a8 00 20  ..... .

```

eth1: <live capture in progress> ... Packets: 15 Displayed: 15 Marked: 0 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

The image shows a Wireshark network traffic capture. The main pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, and Info. Several packets are highlighted in red, indicating retransmissions. The Info column for these packets shows "[TCP Retransmission]" and "[TCP Dup ACK #X]".

No.	Time	Source	Destination	Protocol	Info
23275	2.945006	192.168.10.16	192.168.10.1	TCP	lmtp > 32852 [ACK] Seq=22653361 Ack=1 Win=65519 Len=1460
23276	2.945014	192.168.10.16	192.168.10.1	TCP	lmtp > 32852 [ACK] Seq=22654821 Ack=1 Win=65519 Len=1460
23277	2.945021	192.168.10.1	192.168.10.16	TCP	32852 > lmtp [ACK] Seq=1 Ack=22654821 Win=64240 Len=0
23278	2.945055	192.168.10.16	192.168.10.1	TCP	lmtp > 32852 [ACK] Seq=22656281 Ack=1 Win=65519 Len=1460
23279	2.945063	192.168.10.16	192.168.10.1	TCP	lmtp > 32852 [ACK] Seq=22657741 Ack=1 Win=65519 Len=1460
23280	2.945066	192.168.10.16	192.168.10.1	TCP	lmtp > 32852 [ACK] Seq=22659201 Ack=1 Win=65519 Len=1460
23281	2.945070	192.168.10.1	192.168.10.16	TCP	32852 > lmtp [ACK] Seq=1 Ack=22657741 Win=64240 Len=0
23282	2.945079	192.168.10.1	192.168.10.16	TCP	32852 > lmtp [ACK] Seq=1 Ack=22660661 Win=64240 Len=0
23283	2.945990	192.168.10.16	192.168.10.1	TCP	lmtp > 32852 [ACK] Seq=22660661 Ack=1 Win=65519 Len=1460
23284	2.946040	192.168.10.16	192.168.10.1	TCP	lmtp > 32852 [ACK] Seq=22662121 Ack=1 Win=65519 Len=1460
23285	2.946054	192.168.10.1	192.168.10.16	TCP	32852 > lmtp [ACK] Seq=1 Ack=22663581 Win=64240 Len=0
23286	2.946993	192.168.10.16	192.168.10.1	TCP	lmtp > 32852 [ACK] Seq=22663581 Ack=1 Win=65519 Len=616
23287	2.949710	192.168.10.1	192.168.10.16	TCP	32852 > lmtp [ACK] Seq=1 Ack=22664197 Win=64240 Len=0
23288	3.442696	192.168.10.16	192.168.10.1	TCP	[TCP Retransmission] lmtp > 32852 [ACK] Seq=22631461 Ack=1 Win=65519 Len=1460
23289	3.442717	192.168.10.1	192.168.10.16	TCP	[TCP Dup ACK 23287#1] 32852 > lmtp [ACK] Seq=1 Ack=22664197 Win=64240 Len=0
23290	3.943650	192.168.10.16	192.168.10.1	TCP	[TCP Retransmission] lmtp > 32852 [ACK] Seq=22631461 Ack=1 Win=65519 Len=1460
23291	3.943670	192.168.10.1	192.168.10.16	TCP	[TCP Dup ACK 23287#2] 32852 > lmtp [ACK] Seq=1 Ack=22664197 Win=64240 Len=0
23292	4.444647	192.168.10.16	192.168.10.1	TCP	[TCP Retransmission] lmtp > 32852 [ACK] Seq=22631461 Ack=1 Win=65519 Len=1460
23293	4.444665	192.168.10.1	192.168.10.16	TCP	[TCP Dup ACK 23287#3] 32852 > lmtp [ACK] Seq=1 Ack=22664197 Win=64240 Len=0
23294	4.945621	192.168.10.16	192.168.10.1	TCP	[TCP Retransmission] lmtp > 32852 [ACK] Seq=22631461 Ack=1 Win=65519 Len=1460
23295	4.945637	192.168.10.1	192.168.10.16	TCP	[TCP Dup ACK 23287#4] 32852 > lmtp [ACK] Seq=1 Ack=22664197 Win=64240 Len=0
23296	5.446598	192.168.10.16	192.168.10.1	TCP	[TCP Retransmission] lmtp > 32852 [ACK] Seq=22631461 Ack=1 Win=65519 Len=1460
23297	5.446616	192.168.10.1	192.168.10.16	TCP	[TCP Dup ACK 23287#5] 32852 > lmtp [ACK] Seq=1 Ack=22664197 Win=64240 Len=0
23298	5.947552	192.168.10.16	192.168.10.1	TCP	[TCP Retransmission] lmtp > 32852 [ACK] Seq=22631461 Ack=1 Win=65519 Len=1460
23299	5.947569	192.168.10.1	192.168.10.16	TCP	[TCP Dup ACK 23287#6] 32852 > lmtp [ACK] Seq=1 Ack=22664197 Win=64240 Len=0
23300	5.947676	192.168.10.16	192.168.10.1	TCP	lmtp > 32852 [ACK] Seq=22664197 Ack=1 Win=65519 Len=1460
23301	5.947705	192.168.10.1	192.168.10.16	TCP	32852 > lmtp [ACK] Seq=1 Ack=22665657 Win=64240 Len=0
23302	5.947795	192.168.10.16	192.168.10.1	TCP	lmtp > 32852 [ACK] Seq=22665657 Ack=1 Win=65519 Len=1460 [Packet size limited during c
23303	5.947803	192.168.10.16	192.168.10.1	TCP	lmtp > 32852 [ACK] Seq=22667117 Ack=1 Win=65519 Len=1460
23304	5.947807	192.168.10.16	192.168.10.1	TCP	lmtp > 32852 [ACK] Seq=22668577 Ack=1 Win=65519 Len=1460
23305	5.947811	192.168.10.1	192.168.10.16	TCP	32852 > lmtp [ACK] Seq=1 Ack=22667117 Win=64240 Len=0
23306	5.947818	192.168.10.1	192.168.10.16	TCP	32852 > lmtp [ACK] Seq=1 Ack=22668577 Win=64240 Len=0
23307	5.947828	192.168.10.1	192.168.10.16	TCP	32852 > lmtp [ACK] Seq=1 Ack=22670037 Win=64240 Len=0

Frame 1 (1514 bytes on wire, 74 bytes captured)  
Ethernet II, Src: 02:00:c0:a8:00:10 (02:00:c0:a8:00:10), Dst: IntelCor\_8b:60:13 (00:1b:21:8b:60:13)  
Internet Protocol, Src: 192.168.10.16 (192.168.10.16), Dst: 192.168.10.1 (192.168.10.1)  
Transmission Control Protocol, Src Port: lmtp (74), Dst Port: 32852 (32852), Seq: 1, Ack: 1, Len: 1460

```
0000 00 1b 21 8b 60 13 02 00 c0 a8 00 10 08 00 45 00  ...l... ..E.  
0010 05 dc 2f d8 40 00 80 06 2f e2 c0 a8 0a 10 c0 a8  ../.@... /.....  
0020 0a 01 00 18 80 54 45 80 91 be bc 68 77 cf 50 10  ...TE... ..hw.P.  
0030 ff ef 5a 43 00 00 00 00 00 00 00 00 00 00 00 00  ..ZC.....
```

File: "retry\_0.cap" 16 MB 00:00:29 Packets: 213449 Displayed: 213449 Marked: 0 Profile: Default