

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



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

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

0.0000000.000000connect start (プログラムの出力)0.0003630.000363IP 192.168.0.100.35005 > 192.168.0.101.13: S0.0004890.000126IP 192.168.0.101.13> 192.168.0.100.35005: S0.0005360.000047IP 192.168.0.100.35005 > 192.168.0.101.13: . ack 1 win 14600.0005830.000047connect 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], seg 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 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 Ρ.... 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.... 0000 0000 0000 0000 0000 0000 0000 0x0030: 0x0040: 0x0050: 0x0060:

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)

| - | <u>E</u> dit <u>V</u> iew | <u>G</u> o <u>C</u> apture <u>A</u> | nalyze <u>S</u> tatistics | Telephony <u>T</u> ools | Internals Help |
|---------|---------------------------|-------------------------------------|---------------------------|-------------------------|---------------------------------------|
| • | 🥻 🔳 | 🙇 🗈 🗋 | × 2 °, · | 🗢 👄 😜 孩 | 业 🗏 📑 0, 0, 0, 12 ₩ 12 15 🕺) 第 |
| entror: | | | | | Expression Clear Apply Save |
| No. | Time | Source | Des | stination | Protocol Length Info |

 \mathbb{Q}

◯ 🤎 ローカル エリア接続: <live capture in progress> … No Packets

| <u>F</u> ile | <u>E</u> dit | . <u>V</u> iew | <u>G</u> o <u>C</u> apture | <u>A</u> nalyze <u>S</u> tatistics | Telephony <u>T</u> ools <u>I</u> nt | ternals <u>H</u> elp |
|--------------|--------------|----------------|----------------------------|------------------------------------|-------------------------------------|----------------------------------|
| 0 | ۲ | <i>"</i> | <u>a</u> 🖿 |) × 2 9 | ⇔ ⇔ ⇔ 7 1 | ▙▕▕▇▏ ④, ○, ◎, ♡ ፼ ⊠ 畅 ፠ ፬3 |
| Filter | | | | | 7 | Expression Clear Apply Save |
| No. | 1 | Time | Source | [D | estination | Protocol Length Info |

| | Device | Description | | IP | Packets | Packets/s | |
|----|-----------------------------------|--------------------------------|---------------|----------------------|---------|-----------|-----------------|
| | 🛛 🛃 VMware Network Adapter VMnet8 | VMware Virtual Ethernet Adapte | r | fe80::8c8d:a50a:1654 | k62d2 - | - | <u>D</u> etails |
| | 🛛 🚰 VMware Network Adapter VMnet1 | VMware Virtual Ethernet Adapte | r | fe80::8014:fc9b:f8a2 | :5436 - | - | <u>D</u> etails |
| ┟╒ | 📊 ローカル エリア接続 2 | Broadcom NetXtreme Gigabit Et | hernet Driver | fe80::4997:882:5e7: | 41ae - | - | <u>D</u> etails |
| | 1 🗗 ローカル エリア接続 | Intel(R) PRO/100+ Management | Adapter | fe80::1d22:21ef:36a6 | :66ca - | - | <u>D</u> etails |
| | <u>H</u> elp | | <u>S</u> tart | Stop | Options | s | <u>C</u> lose |

◯ 💅 ローカル エリア接続: <live capture in progress> … ∫ No Packets

Profile: Default

| Filte | r: | | ✓ Expression Clear | Apply Save | 2 | |
|-------|---|----------------|--------------------|--------------|--|-------------|
| No. | Time 🖡 | Source | Destination | Protocol Ler | ngth Info | ^ |
| | ¹ Time (format as specified) | 192.168.10.20 | 192.168.10.102 | TCP | 66 54155 > EtherNet-IP-1 [SYN] Seq=0 Win=1 | _2 = |
| | 2 0.000214 | 192.168.10.102 | 192.168.10.20 | TCP | 66 EtherNet-IP-1 > 54155 [SYN, ACK] Seq=0 | F |
| | 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 | ТСР | 1078 EtherNet-IP-1 > 54155 [PSH, ACK] Seq=1 | Α |
| | 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 | 12 |
| | 7 0.000857 | 192.168.10.20 | 192.168.10.102 | TCP | 54 54155 > EtherNet-IP-1 [ACK] Seq=1 Ack=2 | 20 |
| | 8 0.001026 | 192.168.10.102 | 192.168.10.20 | TCP | 1078 EtherNet-IP-1 > 54155 [PSH, ACK] Seq=20 | 14 |
| | 9 0.001041 | 192.168.10.20 | 192.168.10.102 | TCP | 54 54155 > EtherNet-IP-1 [ACK] Seg=1 Ack=3 | <u>.</u> (~ |
| < | | III | | | > | •] |

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)

..!.`... !S.R..E. 0000 00 lb 21 8b 60 14 00 lb 21 53 b9 52 08 00 45 00 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 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 00 . ~ Packets: 17087 · Displayed: 17087 (100.... Profile: Default File: "buf.1k.cap" 11 MB 00:00:00

DAQ-Middlewareトレーニングコース

| | | 📄 🗶 🛃 🛤 | 🔹 🖈 🏊 🛓 | | . 🖭 👹 🔟 📑 📧 🛛 💿 |
|--|--|---------|---------|--|-----------------|
|--|--|---------|---------|--|-----------------|

| Filter | r: [| | ✓ Expression Clear | Apply Save | e | |
|--------|------------|----------------|--------------------|-------------|--|-----|
| No. | Time | Source | Destination | Protocol Le | ngth Info | ^ |
| | 1 0.000000 | 192.168.10.20 | 192.168.10.102 | TCP | 66 54155 > EtherNet-IP-1 [SYN] Seq=0 Win=1 | 4 = |
| | 2 0.000214 | 192.168.10.102 | 192.168.10.20 | TCP | 66 EtherNet-IP-1 > 54155 [SYN, ACK] Seq=0 | ł |
| | 3 0.000242 | 192.168.10.20 | 192.168.10.102 | TCP | 54 54155 > EtherNet-IP-1 [ACK] Seq=1 Ack=1 | Ē |
| | 4 0.000673 | 192.168.10.102 | 192.168.10.20 | ТСР | 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 | Č |
| | 6 0.000842 | 192.168.10.102 | 192.168.10.20 | TCP | 1078 EtherNet-IP-1 > 54155 [PSH, ACK] Seq=10 | 2 |
| | 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 | 2 |
| | 9 0.001041 | 192.168.10.20 | 192.168.10.102 | TCP | 54 54155 > EtherNet-IP-1 [ACK] Seg=1 Ack=3 | (~ |
| < | | 111 | | | > | 1 |

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 lb | 21 | 8b 6 | 50 14 | | 1b | 21 | 53 | b9 | 52 | | 0 4 | 50 | 0 | ! . ` | | !S.R., E. | | ç |
| 0010 | 04 28 | 6b | e4 4 | 10 00 | J 40 | 06 | 35 | 21 | c0 | a8 / | 0a 6 | 6 c | 0 a | 8 | .(k.@.@. | | 5!f | ≡ | |
| 0020 | 0a 14 | 08 | ae c | 13 8b | ა db ა | d0 | 25 | 81 | a9 ' | 27 | be 2 | 26 5 | 0 1 | .8 | | . 1 | %'.&P. | | |
| 0030 | 00 73 | 3 d0 | b4 0 | 00 00 |) 00 | 00 | 00 | 00 | 00 | 00 | 00 0 | 0 0 | 0 0 | 0 | . S | | | | |
| 0040 | 00 00 | 00 (| 00 0 | 00 00 |) OO | 00 | 00 | 00 | 00 | 00 | 00 0 | 0 0 | 0 0 | 0 | | | | | |
| 0050 | 00 00 | 00 (| 00 0 | 90 00 |) 00 | 00 | 00 | 00 | 00 | 00 | 00 0 | 0 0 | 00 | 0 | | | | | |
| 0060 | 00 00 | 00 (| 00 0 | 00 00 |) 00 | 00 | 00 | 00 | 00 | 00 | 00 0 | 0 0 | 00 | 0 | | | | | |
| 0070 | 00 00 | 00 (| 00 0 | 00 00 |) 00 | 00 | 00 | 00 | 00 | 00 | 00 0 | 0 0 | 0 0 | 0 | | | | | |
| 0080 | 00 00 | 00 | 00 0 | 10 00 | 1 00 | 0.0 | 00 | 00 | 00 | 00 | 00 0 | 0 01 | 0 0 | Ω | | | | 1 | ۲ |
| 0 💅 | Etherr | net (e | eth), | 14 by | ytes | 5 | | | Pac | cket | s: 1 | 7087 | ۰D | ispla | ayed: 1708 | 87 | 37 (100 Profile: Default | | |
| 2022 | -09-20 | q | | | | | | | | | | D | AQ | -Mi | iddlewar | re | eトレーニングコース | 17 | 1 |

| Filter | | | ✓ Expression Clear | Apply Save | e | |
|--------|------------|----------------|--------------------|-------------|--|------|
| No. | Time | Source | Destination | Protocol Le | ngth Info | ^ |
| | 1 0.000000 | 192.168.10.20 | 192.168.10.102 | TCP | 66 54155 > EtherNet-IP-1 [SYN] Seq=0 Win=1 | _2 ≡ |
| | 2 0.000214 | 192.168.10.102 | 192.168.10.20 | TCP | 66 EtherNet-IP-1 > 54155 [SYN, ACK] Seq=0 | ł |
| | 3 0.000242 | 192.168.10.20 | 192.168.10.102 | TCP | 54 54155 > EtherNet-IP-1 [ACK] Seq=1 Ack=1 | L |
| | 4 0.000673 | 192.168.10.102 | 192.168.10.20 | ТСР | 1078 EtherNet-IP-1 > 54155 [PSH, ACK] Seq=1 | 4 |
| | 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 |)2 |
| | 7 0.000857 | 192.168.10.20 | 192.168.10.102 | TCP | 54 54155 > EtherNet-IP-1 [ACK] Seq=1 Ack=2 | 20 |
| | 8 0.001026 | 192.168.10.102 | 192.168.10.20 | TCP | 1078 EtherNet-IP-1 > 54155 [PSH, ACK] Seq=20 |)2 |
| | 9 0.001041 | 192.168.10.20 | 192.168.10.102 | TCP | 54 54155 > EtherNet-IP-1 [ACK] Seg=1 Ack=3 | 3(🗠 |
| < | | 111 | | | | • |

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 , 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 <mark>45 00</mark> !.` !S.R <mark>E.</mark> | <u>^</u> |
|------|---|----------|
| 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 00 | |
| 0040 | $00 \ 00 \ 00 \ 00 \ 00 \ 00 \ 00 \ 00 $ | |
| 0050 | $00 \ 00 \ 00 \ 00 \ 00 \ 00 \ 00 \ 00 $ | |
| 0060 | $00 \ 00 \ 00 \ 00 \ 00 \ 00 \ 00 \ 00 $ | |
| 0070 | $00 \ 00 \ 00 \ 00 \ 00 \ 00 \ 00 \ 00 $ | |
| 0080 | | L~ |
| 0 💅 | Internet Protocol Version 4 (ip), 2 🗄 Packets: 17087 · Displayed: 17087 (100 🗄 Profile: Default | |
| | | |

DAQ-Middlewareトレーニングコース

| • • | | 🖴 🗋 🗙 🛃 🛱 | 🔹 🔿 春 👱 | | 1 |
|-----|--|-----------|---------|--|---|
|-----|--|-----------|---------|--|---|

| Filte | r: | | ✓ Expression Clear | Apply Save | e | |
|-------|------------|----------------|--------------------|-------------|--|------|
| No. | Time | Source | Destination | Protocol Le | ngth Info | ^ |
| | 1 0.000000 | 192.168.10.20 | 192.168.10.102 | ТСР | 66 54155 > EtherNet-IP-1 [SYN] Seq=0 Win=1 | .∠ = |
| | 2 0.000214 | 192.168.10.102 | 192.168.10.20 | TCP | 66 EtherNet-IP-1 > 54155 [SYN, ACK] Seq=0 | F |
| | 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 | ТСР | 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 | 2 |
| | 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 | 2 |
| | 9 0.001041 | 192.168.10.20 | 192.168.10.102 | TCP | 54 54155 > EtherNet-IP-1 [ACK] Seg=1 Ack=3 | (~ |
| < | | 111 | | | > | - |

k

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 | | |
| 0050 | 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 | |
| 0070 | | |
| 0080 | 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 | |
| 0020 | | |
|) 🎽 | ransmission Control Protocol (tc Packets: 17087 · Displayed: 17087 (100 Profile: Default | |

| File | Edit | View Go |) Cap | oture | e Ana | alyze | Statis | tics T | elepho | ony | Tools | Inter | nals | Help | ~ ~ | ~ | | | | | | _ |
|----------------|--------------|--------------------------|----------------|--------------|----------------|---------------|------------------|---------------|----------------|----------------|---------------|------------------|----------------|-------------------|----------|----------------|----------------|--------|---------------|----------|-------|----------|
| | 0 | | J | E | | × | 2 | 19 | - | | • | | | | e, e | |) + | Ŭ. | ¥ | | 9 | 9 |
| Filter | | | | | | | | | | ~ | Expre | ession | . Cle | ear Apply | Save | | | | | | | |
| No. | Tir | me | | | | Sou | rce | | | De | stinat | tion | | Protocol | Length | Info | | | | | | |
| | 10. | 000000 | | | | 192. | 168.1 | 9.20 | | 192 | . 168 | . 10. 10 | 2 | TCP | 66 | 54155 | i > Etl | herNet | -IP-1 | [SYN] | Seq=0 | Win=14 |
| | 20. | 000214 | | | | 192. | 168.1 | 9.102 | | 192 | . 168 | . 10.20 | | TCP | 66 | Ether | Net-I | P-1 > | 54155 | [SYN, | ACK] | Seq=0 / |
| | 30. | 000242 | | | | 192. | 168.1 | 9.20 | | 192 | . 168 | . 10. 10 | 2 | TCP | 54 | 54155 | i > Etl | herNet | -IP-1 | [ACK] | Seq=1 | . Ack=1 |
| | 40. | 000673 | | | | 192. | 168.1 | 9.102 | | 192 | . 168 | . 10. 20 | 2 | TCP | 1078 | Ether | Net-I | P-1 > | 54155 | [PSH, | ACK | Seq=1 / |
| | 50. | 000692 | | | | 192. | 168.1 | 9.20 | | 192 | . 168 | . 10. 10 | 2 | TCP | 1079 | 54155 Ethor |) > ETI | nerwet | - 1P - 1 | [ACK] | Seq=1 | . ACK=10 |
| | 00. 70 | 000842 | | | | 102 | 160 1 | 9.10Z | | 102 | 160 | 10.20 | 2 | TCP | 1078 | 54155 | Net-11 | P-L > | 04100 тр 1 | [PSH, | ACK J | Seq=102 |
| | 70. 80 | 0000007 | | | | 192. | 168 1 | 0.20 0.100 | | 192 | 168 | 10.10 | 2 | TCP | 1078 | Ether | -Not-TI | | 54155 | [ACK] | VCKJ | Sea-20/ |
| | 90. 90. | 001020 | | | | 192. | 168.1 | 9.20 | | 192 | 168 | 10.20 | 2 | TCP | 54 | 54155 | | herNet | -TP-1 | [ACK] | Sed=1 | Ack=3(|
| < | | 001041 | | | | 1.77 | 1007.1 | | | 1.77 | | | | 1 | | | | | | 1712.111 | | > |
| Þ Fra Þ Eth | me 4 erne | 4: 1078 by et II, Src | tes d : Int | on w telC | ire (or_53 | 8624 :b9:5 | bits), 2 (00: | 1078 1b:21 | byte: 53:b9 | s cap 9:52) | oture , Ds | d (862 t: Int | 24 bi telCo | ts) r_8b:60:14 | (00:1b:2 | 21:8b: | 60:14) |) | | | | |
| ⊳ Int | erne | et Protoco | ol Ve | rsio | n 4, | Src: | 192.16 | 8.10. | 102 (1 | 192.1 | 68.1 | 0.102) | , Ds | t: 192.168. | 10.20 (1 | L92.16 | 8.10.2 | 20) | | | | |
| ⊳ Tra | nsmi | ission Con | ntrol | Pro | tocol | , Src | Port: | Ethe | rNet-1 | [P-1 | (222 | 2), Ds | st Po | rt: 54155 (| 54155), | Seq: | 1, Ac | k: 1, | Len : | 1024 | | |
| ▼ Dat | a (1 | 1024 bytes | 5) | | | | | | | | | | <u> </u> | | | | | | | | | |
| 0 | ata | : 00000000 | 00000 | 0000 | 00000 | 00000 | 000000 | 00000 | 00000 | 00000 | 30 | | ~ | | | | | | | | | |
| [| Leng | gth: 1024] |] | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |
| 0000 | 00 | 1b 21 8b | 60 14 | 1 00 | 1b | 21 53 | b9 52 | 08 00 |) 45 0 | 0 | !.` | ` I | S.R | Ε. | | | | | | | | |
| 1010 | 04 | 28 6b e4 | 40 00 | 1 40 | 06 | 35 21 | C0 a8 | 0a 66 |) CO a | 8 | . (K. (| a.a. 5 | 11 | F | | | | | | | | |

| 0010 | 04 20 00 64 40 | 00 40 00 | JJ 2 | 1 00 | ao 0a | 00 | 0.0 | ao | . (| J: | | = |
|-------|------------------------|-----------------|-------|--------------|--------|-----|------|-------|------------|--------|------------------|--------------|
| 0020 | 0a 14 08 ae d3 | 8b db d0 | 25 8 | 31 a9 | 27 be | 26 | 50 | 18 | | %'.&P. | | |
| 0030 | 00 73 d0 b4 00 | 00 00 00 | 00 0 | 00 00 | 00 00 | 00 | 00 | 00 | . s | | | |
| 0040 | 00 00 00 00 00 | 00 00 00 | | 00 00 | | | | 00 | | | | |
| 0050 | 00 00 00 00 00 | | | 00 00 | | | | 00 | | | | |
| 0060 | 00 00 00 00 00 | | | 00 00 | | | | 00 | | | | |
| 0070 | 00 00 00 00 00 | | | 00 00 | | | | 00 | | | | |
| 0080 | <u> </u> | <u>00 00 00</u> | 0.0.0 | <u>10 00</u> | 00 00 | 00 | 00 | 00 | | | | \mathbf{r} |
|) 🔰 | Data (data), 1024 | bytes | | Pa | ckets: | 170 | 87 · | Displ | ayed: 1708 | 7 (100 | Profile: Default | |
| 2022- | 09-29 | | | | | | DA | Q-M | iddleware | eトレーニ | ングコース 2 | 20 |

| <u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture | Analyze Statistics Telephony Tools Help | | | | | | | | |
|---|--|--|--|--|--|--|--|--|--|
| | Display Filters | | | | | | | | |
| | Display Filter <u>M</u> acros | | | | | | | | |
| Filter: tcp.stream eq 0 | Clear Apply | | | | | | | | |
| | Appig as filter | | | | | | | | |
| No Time | Prepare a Filter > Protocol Info | | | | | | | | |
| 21 19.262914 | Enabled Protocols Shift+Ctrl+E | | | | | | | | |
| 22 19.263081 | C Enabled Protocols Shift ctitle 31 TCP tell | | | | | | | | |
| 23 19.263107 | C3 Decode As 2 ICP 447 | | | | | | | | |
| 24 19.200894 | दे <u>ः U</u> ser Specified Decodes | | | | | | | | |
| 25 19.265361 | | | | | | | | | |
| 27 19 266206 | Follow ICP Stream 2 TCP 447 | | | | | | | | |
| 28 19, 266265 | Follow UDP Stream | | | | | | | | |
| 29 19.266284 | Follow SSL Stream 2 TCP 447 | | | | | | | | |
| 30 19.267863 | Expert Info 01 TELNET Telr | | | | | | | | |
| 31 19.267952 | P Expert Info Composite 2 TCP 447 | | | | | | | | |
| 32 19.268015 | 2 TELNET Teli | | | | | | | | |
| 33 19.268052 | Conversation Hiter > 01 TCP teli | | | | | | | | |
| 24 10 260772 | | | | | | | | | |
| | | | | | | | | | |
| Frame 24 (62 bytes on wir b fill | e, 62 bytes captured) | | | | | | | | |
| Ethernet II, Src: IntelCo | r_8b:60:14 (00:1b:21:8b:60:14), Dst: 02:00:c0:a8:00:20 (02:00:c0:a | | | | | | | | |
| P Internet Protocol, Src: 1 | 92.168.0.101 (192.168.0.101), DST: 192.168.0.32 (192.168.0.32) | | | | | | | | |
| P Transmission Control Prot N Talact | ocol, Src Port: 44/// (44///), Dst Port: telhet (23), Seq: 1, Ack: | | | | | | | | |
| V Telhet | | | | | | | | | |
| < | | | | | | | | | |
| 0000 02 00 c0 a8 00 20 00 1 | Lb 21 8b 60 14 08 00 45 00 !.`E. | | | | | | | | |
| 0010 00 30 2e 9f 40 00 40 0 | 06 8a 53 c0 a8 00 65 c0 a8 .0@.@Se | | | | | | | | |
| 0020 00 20 ae e9 00 17 ac 7 | 76 a0 3a e5 9b ca fd 50 18v.:P. | | | | | | | | |
| 0030 39 08 81 f8 00 00 a3 0 | 00 00 00 00 40 00 9 @. | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| Talact (talact) Olympic 20 Diselects 00 Diselected CO Marked Constants Diselected | | | | | | | | | |

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

<u>File Edit View Go Capture Analyze Statistics Telephony</u> Tools <u>H</u>elp

🗒 🍓 🍭 🌬 i 🖴 🚾 🗶 🥩 📥 i 🗛 💠 🌩 🏊 🛨 i 🗐 🕞 i 🍳 🔍 🕾 i 🕁 😢 🐻 i 👼

| Filter: | | ~ | Expression Clear App | ly | | |
|-----------------|--------------------------------|-----------------------|-----------------------|------------|---|------|
| 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 | Ξ |
| 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 | 2.949693 | 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 | <pre>lmtp > 32852 [ACK] Seq=22665657 Ack=1 Win=65519 Len=1460[Packet size limited during</pre> | 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 | hytes cantured) | | | | |
| b Etherr | 1 (1514 5)(05 00 wire, 74 | 10 (02.00.c0.a8.00.10 |) Det. IntelCor 8b.60 | 0.13 (00.1 | 1h · 21 · 8h · 60 · 13) | = |
| > Inter | net Protocol Src, 102 169 | | Det: 102 169 10 1 /10 | 07 160 10 | 1) | - |
| N Transr | niccion Control Drotocol C | re Dort, 1mtp (24) D | DSC. 152.100.10.1 (1: | 52.100.10. | Ack, 1 Jan, 1460 | ~ |
| | The product of the protocol. S | | | . seu: 1. | ALK: 1. LEN: 1400 | |
| 19191414 (4)(4) | | 48 00 10 08 00 45 00 | I F | | | 11.0 |

File: "retry_0.cap" 16 MB 00:00:29 Packets: 213449 Displayed: 213449 Marked: 0

DAQ-Middlewareトレーニングコース

Profile: Default