



Network 2

情報セキュリティ・スキルアッププロジェクト



を中心にネットワークに触れていきます

Wireshark とは

ネットワークを流れるデータをキャプチャ
したりそれを解析したりできるツール

通信は目に見えない

Wiresharkを使用することで
通信状況を可視化することができる

とりあえず、使ってみよう



開く

C:\Users\nakaya39\Desktop\ctf4b\record.pcap (751 Bytes)
 C:\Users\nakaya39\Desktop\folder\secPRJ\ctf4b_講義_network\sample\sample.pcap (35 KB)
 C:\tsark_capture\Packet_Data\output_00001_202303080025.pcapng (3576 KB)
 C:\Users\nakaya39\Desktop\Packet Street\Packet_Data\output_00022_20230304134959.pcapng (見つかりません)
 C:\Users\nakaya39\Desktop\Packet Street\Packet_Data\output_00020_20230304134953.pcapng (見つかりません)
 C:\Users\nakaya39\Desktop\ctf4bgl\quiz_mid3.pcap (見つかりません)
 C:\Users\nakaya39\Desktop\CTFワークショップ\log.pcap (見つかりません)
 C:\Users\nakaya39\Desktop\CTFワークショップ\Sample\log.pcap (見つかりません)
 C:\Users\nakaya39\Desktop\新しいフォルダー\http_data.pcapng (2800 Bytes)
 C:\Users\nakaya39\Desktop\http_data.pcapng (見つかりません)

キャプチャ

…このフィルタを利用:

すべての表示されたインターフェース

- ☒ Wi-Fi 
- ☐ Adapter for loopback traffic capture 
- ☐ ローカル エリア接続* 10
- ☐ ローカル エリア接続* 9
- ☐ ローカル エリア接続* 8
- ☐ Bluetooth ネットワーク接続
- ☐ VMware Network Adapter VMnet8
- ☐ VMware Network Adapter VMnet1
- ☐ ローカル エリア接続* 13
- ☐ ローカル エリア接続* 7

学習

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord

Wiresharkを起動中4.0.1 (v4.0.1-0-ge9f3970b1527).自動アップデートを受信します

Wi-Fi

ファイル(F) 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(T) ヘルプ(H)

表示フィルタ ... <Ctrl-/> を適用

o.

Time

Source

Destination

Cookie pair

Protocol

Length

Source Port

Key

Info

| | | | | | | | | | |
|-----|----------|-------------------|-----------------|--|----------|-----|-------|--|---|
| 99 | 2.196648 | 172.18.5.108 | 172.18.7.255 | | NBNS | 92 | | | Name query NB 0B685F000000<00> |
| 100 | 2.297586 | Chongqin_cb:6a:43 | Broadcast | | ARP | 60 | | | Who has 172.18.4.125? Tell 172.18.7.6 |
| 101 | 2.297586 | IntelCor_d6:96:5b | Broadcast | | ARP | 60 | | | Who has 192.168.11.1? Tell 172.18.4.3 |
| 102 | 2.297586 | IntelCor_d7:4f:0b | Broadcast | | ARP | 60 | | | Who has 192.168.3.1? Tell 172.18.4.209 |
| 103 | 2.297586 | 0.0.0.0 | 255.255.255.255 | | DHCP | 342 | | | DHCP Discover - Transaction ID 0x45447a29 |
| 104 | 2.301620 | 76:90:59:95:86:68 | Broadcast | | ARP | 60 | | | Who has 169.254.64.250? (ARP Probe) |
| 105 | 2.361285 | 172.18.5.109 | 202.13.170.204 | | TCP | 108 | 52917 | | 52917 → 8080 [PSH, ACK] Seq=1 Ack=1 Win=511 Len=54 |
| 106 | 2.412185 | Apple_5b:b5:2d | Broadcast | | ARP | 64 | | | Gratuitous ARP for 172.18.6.145 (Request) |
| 107 | 2.425310 | 202.13.170.204 | 172.18.5.109 | | TCP | 110 | 8080 | | 8080 → 52917 [PSH, ACK] Seq=1 Ack=55 Win=51100 Len=56 |
| 108 | 2.469646 | 172.18.5.109 | 202.13.170.204 | | TCP | 54 | 52917 | | 52917 → 8080 [ACK] Seq=55 Ack=57 Win=511 Len=0 |
| 109 | 2.506507 | IntelCor_4d:6f:16 | Broadcast | | ARP | 60 | | | Who has 172.18.7.254? Tell 172.18.4.16 |
| 110 | 2.506507 | IntelCor_e4:b5:ba | Broadcast | | ARP | 60 | | | Who has 172.18.7.254? Tell 172.18.5.81 |
| 111 | 2.506507 | 172.18.7.245 | 172.18.7.255 | | NBNS | 92 | | | Name query NB BRW2C6FC94C74F6<00> |
| 112 | 2.506507 | 172.18.4.208 | 172.18.7.255 | | UDP | 305 | | | 54915 → 54915 Len=263 |
| 113 | 2.514500 | IntelCor_85:07:af | Broadcast | | ARP | 60 | | | Who has 172.18.7.254? Tell 172.18.6.164 |
| 114 | 2.514500 | IntelCor_e6:22:2e | Broadcast | | ARP | 60 | | | Who has 172.18.4.68? Tell 172.18.5.13 |
| 115 | 2.514500 | 172.18.5.108 | 255.255.255.255 | | DB-LS... | 488 | | | Dropbox LAN sync Discovery Protocol, JavaScript Object Notation |
| 116 | 2.610944 | 172.18.5.108 | 255.255.255.255 | | DB-LS... | 527 | | | Dropbox LAN sync Discovery Protocol, JavaScript Object Notation |
| 117 | 2.610944 | IntelCor_e1:64:5a | Broadcast | | ARP | 60 | | | Who has 172.18.4.68? Tell 172.18.6.73 |
| 118 | 2.610944 | IntelCor_de:49:0a | Broadcast | | ARP | 60 | | | Who has 192.168.2.1? Tell 172.18.7.33 |
| 119 | 2.614426 | IntelCor_c4:ef:46 | Broadcast | | ARP | 60 | | | Who has 192.168.10.1? Tell 172.18.4.121 |
| 120 | 2.614426 | 172.18.4.68 | 172.18.7.255 | | NBNS | 110 | | | Registration NB LAPTOP-D03MKE76<20> |
| 121 | 2.614426 | IntelCor_86:e2:05 | Broadcast | | ARP | 60 | | | Who has 172.18.4.68? Tell 172.18.4.60 |
| 122 | 2.715506 | IntelCor_b8:a7:1d | Broadcast | | ARP | 60 | | | Who has 172.18.4.68? Tell 172.18.5.229 |
| 123 | 2.719960 | IntelCor_dc:33:86 | Broadcast | | ARP | 60 | | | Who has 172.18.4.68? Tell 172.18.5.110 |
| 124 | 2.719960 | IntelCor_d6:55:ec | Broadcast | | ARP | 60 | | | ARP Announcement for 172.18.7.198 |
| 125 | 2.819796 | IntelCor_ff:12:75 | Broadcast | | ARP | 60 | | | Who has 172.18.4.68? Tell 172.18.7.41 |
| 126 | 2.819796 | IntelCor_19:36:a1 | Broadcast | | ARP | 60 | | | Who has 172.18.4.68? Tell 172.18.6.214 |

Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{F66897E2-5AF4-4ED8-8026-166E2AEF9BDE}, id 0

Ethernet II, Src: IntelCor_de:49:0a (f0:57:a6:de:49:0a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Address Resolution Protocol (request)

0000

0010

0020

0030

パケットとは？

インターネットなどTCP/IPネットワークで通信を行う際、データはIP（Internet Protocol）によって分割される。

この分割されたデータのことをパケットと呼ぶ。

これ一つ一つがパケット

| | | | | | |
|-----|----------|-------------------|-----------------|----------|-----------|
| 103 | 2.297586 | 0.0.0.0 | 255.255.255.255 | DHCP | 342 |
| 104 | 2.301620 | 76:90:59:95:86:68 | Broadcast | ARP | 60 |
| 105 | 2.361285 | 172.18.5.109 | 202.13.170.204 | TCP | 108 52917 |
| 106 | 2.412185 | Apple_5b:b5:2d | Broadcast | ARP | 64 |
| 107 | 2.425310 | 202.13.170.204 | 172.18.5.109 | TCP | 110 8080 |
| 108 | 2.469646 | 172.18.5.109 | 202.13.170.204 | TCP | 54 52917 |
| 109 | 2.506507 | IntelCor_4d:6f:16 | Broadcast | ARP | 60 |
| 110 | 2.506507 | IntelCor_e4:b5:ba | Broadcast | ARP | 60 |
| 111 | 2.506507 | 172.18.7.245 | 172.18.7.255 | NBNS | 92 |
| 112 | 2.506507 | 172.18.4.208 | 172.18.7.255 | UDP | 305 |
| 113 | 2.514500 | IntelCor_85:07:af | Broadcast | ARP | 60 |
| 114 | 2.514500 | IntelCor_e6:22:2e | Broadcast | ARP | 60 |
| 115 | 2.514500 | 172.18.5.108 | 255.255.255.255 | DB-LS... | 488 |
| 116 | 2.610944 | 172.18.5.108 | 255.255.255.255 | DB-LS... | 527 |
| 117 | 2.610944 | IntelCor_e1:64:5a | Broadcast | ARP | 60 |

パケットには最大サイズがあり、
一般的には1500bytesとなっている

パケットの最大サイズを
MTU(Maximum Transmission Unit)と呼ぶ

| Destination | Cookie pair | Protocol | Length | Source Port | Key |
|-----------------|-------------|----------|--------|-------------|-----|
| 172.18.7.255 | | NBNS | 92 | | |
| Broadcast | | ARP | 60 | | |
| Broadcast | | ARP | 60 | | |
| Broadcast | | ARP | 60 | | |
| 255.255.255.255 | | DHCP | 342 | | |
| Broadcast | | ARP | 60 | | |
| 202.13.170.204 | | TCP | 1085 | 2917 | |
| Broadcast | | ARP | 64 | | |
| 172.18.5.109 | | TCP | 1108 | 8080 | |
| 202.13.170.204 | | TCP | 545 | 2917 | |
| Broadcast | | ARP | 60 | | |
| Broadcast | | ARP | 60 | | |
| 172.18.7.255 | | NBNS | 92 | | |
| 172.18.7.255 | | UDP | 305 | | |
| Broadcast | | ARP | 60 | | |
| Broadcast | | ARP | 60 | | |
| 255.255.255.255 | | DB-LS... | 488 | | |
| 255.255.255.255 | | DB-LS... | 527 | | |
| Broadcast | | ARP | 60 | | |
| Broadcast | | ARP | 60 | | |
| Broadcast | | ARP | 60 | | |
| 172.18.7.255 | | NBNS | 110 | | |
| Broadcast | | ARP | 60 | | |
| Broadcast | | ARP | 60 | | |

Lengthが
パケットサイズ

TCP/IPとは？

インターネットにおいて広く標準的に
利用されている通信プロトコルのこと

プロトコルとは？

プロトコル = 決まりごと

プロトコルとは？

| Time | Source | Destination | Protocol | Length | Sequence | Details |
|------|----------|----------------|----------------|--------|----------|---|
| 58 | 1.418205 | 202.13.170.204 | 172.18.5.109 | TCP | 110 8080 | 8080 → 52041 [PSH, ACK] Seq=1 Ack=55 Win=51100 Len=56 |
| 59 | 1.419462 | 202.13.170.204 | 172.18.5.109 | TCP | 110 8080 | 8080 → 52036 [PSH, ACK] Seq=1 Ack=55 Win=51100 Len=56 |
| 60 | 1.419462 | 202.13.170.204 | 172.18.5.109 | TCP | 110 8080 | 8080 → 52068 [PSH, ACK] Seq=1 Ack=55 Win=51100 Len=56 |
| 61 | 1.419462 | 202.13.170.204 | 172.18.5.109 | TCP | 60 8080 | 8080 → 52040 [ACK] Seq=1 Ack=55 Win=51100 Len=0 |
| 62 | 1.458433 | 202.13.170.204 | 172.18.5.109 | TCP | 110 8080 | 8080 → 52040 [PSH, ACK] Seq=1 Ack=55 Win=51100 Len=56 |
| 63 | 1.459446 | 172.18.5.109 | 202.13.170.204 | TCP | 54 52041 | 52041 → 8080 [ACK] Seq=55 Ack=57 Win=511 Len=0 |
| 64 | 1.459558 | 172.18.5.109 | 202.13.170.204 | TCP | 54 52036 | 52036 → 8080 [ACK] Seq=55 Ack=57 Win=511 Len=0 |
| 65 | 1.459617 | 172.18.5.109 | 202.13.170.204 | TCP | 54 52068 | 52068 → 8080 [ACK] Seq=55 Ack=57 Win=254 Len=0 |

Frame 58: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on
Ethernet II, Src: Cisco_82:42:80 (70:db:98:82:42:80), Dst: IntelCor_4c:
Internet Protocol Version 4, Src: 202.13.170.204, Dst: 172.18.5.109
Transmission Control Protocol, Src Port: 8080, Dst Port: 52041, Seq: 1,

| | | |
|------|---|-------------------|
| 0000 | 40 1c 83 4c 12 60 70 db 98 82 42 80 08 00 45 00 | @...L.p...B...E. |
| 0010 | 00 60 5a 10 00 00 fe 06 3c 2e ca 0d aa cc ac 12 | ..Z.....<..... |
| 0020 | 05 6d 1f 90 cb 49 54 a2 0b 04 1e 14 89 4c 50 18 | .m...IT...LP. |
| 0030 | c7 9c cc b5 00 00 17 03 03 00 33 66 bd c3 3c bf |3f...< |
| 0040 | 0f 99 4e 31 12 01 da 2c 0d c9 21 c4 eb 82 c8 26 | ..N1...!...& |
| 0050 | 3f ab 44 58 01 e3 24 d9 a6 4b fd bf b3 5a 31 9a | ?DX...\$..K...Z1. |
| 0060 | 01 d4 ba 7f 26 b0 2f 65 20 5d 40 db e6 8a |&/e]@... |

コンピュータが通信を行う場合、
全てのデータは0と1で表される

プロトコルとは？

データの形式ややりとりの順番など
それぞれのコンピュータで把握して
おかなければ通信ができない！

TCP/IPのプロトコル

| | Time | Source | Destination | Cookie pair | Protocol | Length | Source Port | Key |
|----|----------|-------------------|-----------------|-------------|----------|--------|-------------|-----|
| 57 | 1.357640 | 172.18.4.68 | 172.18.7.255 | | STEAM... | 83 | | |
| 58 | 1.418205 | 202.13.170.204 | 172.18.5.109 | | TCP | 110 | 8080 | |
| 59 | 1.419462 | 202.13.170.204 | 172.18.5.109 | | TCP | 110 | 8080 | |
| 60 | 1.419462 | 202.13.170.204 | 172.18.5.109 | | TCP | 110 | 8080 | |
| 61 | 1.419462 | 202.13.170.204 | 172.18.5.109 | | TCP | 60 | 8080 | |
| 62 | 1.458433 | 202.13.170.204 | 172.18.5.109 | | TCP | 110 | 8080 | |
| 63 | 1.459446 | 172.18.5.109 | 202.13.170.204 | | TCP | 54 | 52041 | |
| 64 | 1.459558 | 172.18.5.109 | 202.13.170.204 | | TCP | 54 | 52036 | |
| 65 | 1.459617 | 172.18.5.109 | 202.13.170.204 | | TCP | 54 | 52068 | |
| 66 | 1.460978 | 0.0.0.0 | 255.255.255.255 | | DHCP | 342 | | |
| 67 | 1.460978 | Apple_33:b9:53 | Broadcast | | ARP | 60 | | |
| 68 | 1.462060 | IntelCor_e4:b5:ba | Broadcast | | ARP | 60 | | |
| 69 | 1.462060 | IntelCor_0f:b2:66 | Broadcast | | ARP | 60 | | |
| 70 | 1.505350 | 172.18.5.109 | 202.13.170.204 | | TCP | 54 | 52040 | |
| 71 | 1.566619 | IntelCor_d6:96:5b | Broadcast | | ARP | 60 | | |
| 72 | 1.566619 | Chongqin_dc:31:1d | Broadcast | | ARP | 60 | | |
| 73 | 1.576591 | 172.18.7.203 | 172.18.7.255 | | NBNS | 92 | | |
| 74 | 1.576591 | IntelCor_44:4c:24 | Broadcast | | ARP | 60 | | |
| 75 | 1.576591 | IntelCor_e1:92:f4 | Broadcast | | ARP | 60 | | |
| 76 | 1.577400 | Apple_33:b9:53 | Broadcast | | ARP | 60 | | |

TCP/IPの構造

4層構成



データ送受信の流れ



送信側



受信側

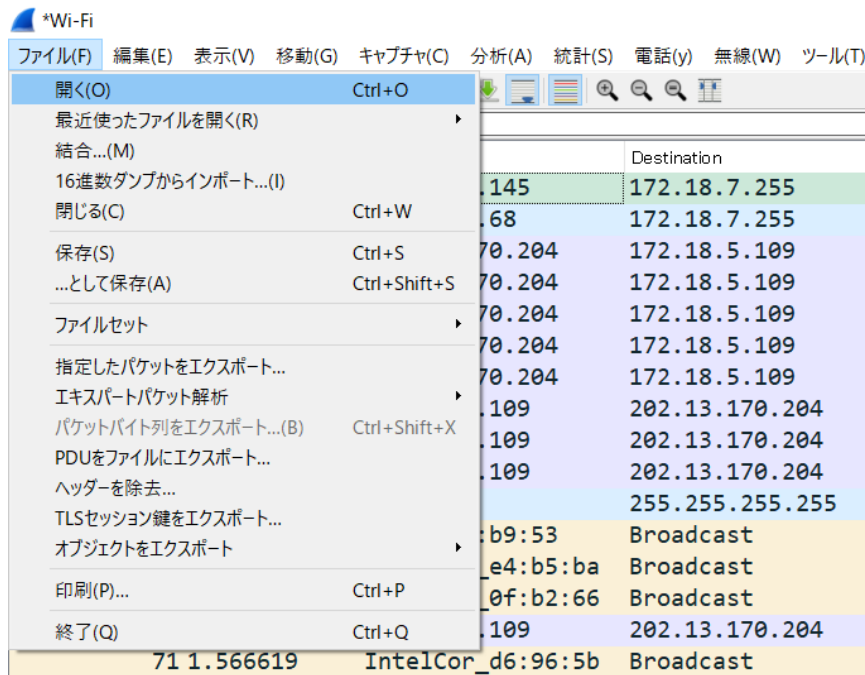


HTTPパケットの層を確認する

<https://wiki.wireshark.org/uploads/27707187aeb30df68e70c8fb9d614981/http.cap>

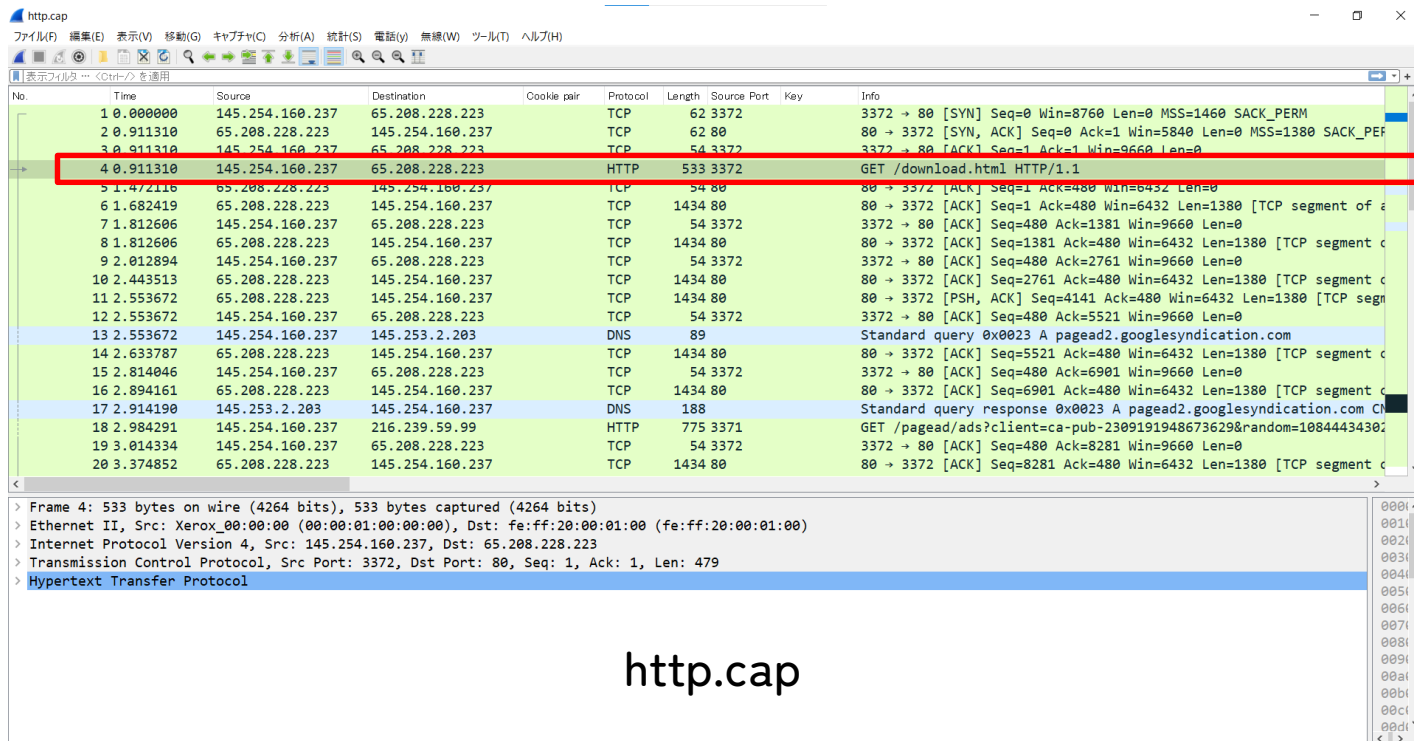
ここからhttp.capをダウンロード

HTTPパケットの層を確認する



右上の「ファイル」→「開く」から
http.capを選択

HTTPパケットの層を確認する



The image shows a Wireshark packet capture analysis of a file named 'http.cap'. The main packet list pane displays a table of captured packets. Packet 4, at time 0.911310, is highlighted with a red box. It is an HTTP GET request from 145.254.160.237 to 65.208.228.223 on port 3372, requesting '/download.html' using HTTP/1.1. The packet details pane below shows the hierarchical structure of the packet: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The packet bytes pane on the right shows the raw data in hexadecimal and ASCII.

| No. | Time | Source | Destination | Cookie pair | Protocol | Length | Source Port | Key | Info |
|-----|----------|-----------------|-----------------|-------------|----------|--------|-------------|-----|--|
| 1 | 0.000000 | 145.254.160.237 | 65.208.228.223 | | TCP | 62 | 3372 | | 3372 → 80 [SYN] Seq=0 Win=8760 Len=0 MSS=1460 SACK_PERM |
| 2 | 0.911310 | 65.208.228.223 | 145.254.160.237 | | TCP | 62 | 80 | | 80 → 3372 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM |
| 3 | 0.911310 | 145.254.160.237 | 65.208.228.223 | | TCP | 54 | 3372 | | 3372 → 80 [ACK] Seq=1 Ack=1 Win=9660 Len=0 |
| 4 | 0.911310 | 145.254.160.237 | 65.208.228.223 | | HTTP | 533 | 3372 | | GET /download.html HTTP/1.1 |
| 5 | 1.472116 | 65.208.228.223 | 145.254.160.237 | | TCP | 54 | 80 | | 80 → 3372 [ACK] Seq=1 Ack=480 Win=6432 Len=0 |
| 6 | 1.682419 | 65.208.228.223 | 145.254.160.237 | | TCP | 1434 | 80 | | 80 → 3372 [ACK] Seq=1 Ack=480 Win=6432 Len=1380 [TCP segment of a |
| 7 | 1.812606 | 145.254.160.237 | 65.208.228.223 | | TCP | 54 | 3372 | | 3372 → 80 [ACK] Seq=480 Ack=1381 Win=9660 Len=0 |
| 8 | 1.812606 | 65.208.228.223 | 145.254.160.237 | | TCP | 1434 | 80 | | 80 → 3372 [ACK] Seq=1381 Ack=480 Win=6432 Len=1380 [TCP segment c |
| 9 | 2.012894 | 145.254.160.237 | 65.208.228.223 | | TCP | 54 | 3372 | | 3372 → 80 [ACK] Seq=480 Ack=2761 Win=9660 Len=0 |
| 10 | 2.443513 | 65.208.228.223 | 145.254.160.237 | | TCP | 1434 | 80 | | 80 → 3372 [ACK] Seq=2761 Ack=480 Win=6432 Len=1380 [TCP segment c |
| 11 | 2.553672 | 65.208.228.223 | 145.254.160.237 | | TCP | 1434 | 80 | | 80 → 3372 [PSH, ACK] Seq=4141 Ack=480 Win=6432 Len=1380 [TCP segn |
| 12 | 2.553672 | 145.254.160.237 | 65.208.228.223 | | TCP | 54 | 3372 | | 3372 → 80 [ACK] Seq=480 Ack=5521 Win=9660 Len=0 |
| 13 | 2.553672 | 145.254.160.237 | 145.253.2.203 | | DNS | 89 | | | Standard query 0x0023 A pagead2.googlesyndication.com |
| 14 | 2.633787 | 65.208.228.223 | 145.254.160.237 | | TCP | 1434 | 80 | | 80 → 3372 [ACK] Seq=5521 Ack=480 Win=6432 Len=1380 [TCP segment c |
| 15 | 2.814046 | 145.254.160.237 | 65.208.228.223 | | TCP | 54 | 3372 | | 3372 → 80 [ACK] Seq=480 Ack=6901 Win=9660 Len=0 |
| 16 | 2.894161 | 65.208.228.223 | 145.254.160.237 | | TCP | 1434 | 80 | | 80 → 3372 [ACK] Seq=6901 Ack=480 Win=6432 Len=1380 [TCP segment c |
| 17 | 2.914190 | 145.253.2.203 | 145.254.160.237 | | DNS | 188 | | | Standard query response 0x0023 A pagead2.googlesyndication.com CN |
| 18 | 2.984291 | 145.254.160.237 | 216.239.59.99 | | HTTP | 775 | 3371 | | GET /pagead/ads?client=ca-pub-2309191948673629&random=1084443430 |
| 19 | 3.014334 | 145.254.160.237 | 65.208.228.223 | | TCP | 54 | 3372 | | 3372 → 80 [ACK] Seq=480 Ack=8281 Win=9660 Len=0 |
| 20 | 3.374852 | 65.208.228.223 | 145.254.160.237 | | TCP | 1434 | 80 | | 80 → 3372 [ACK] Seq=8281 Ack=480 Win=6432 Len=1380 [TCP segment c |

Frame 4: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits)
Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
Internet Protocol Version 4, Src: 145.254.160.237, Dst: 65.208.228.223
Transmission Control Protocol, Src Port: 3372, Dst Port: 80, Seq: 1, Ack: 1, Len: 479
Hypertext Transfer Protocol

http.cap

HTTPパケットの層を確認する

| | | | | | | |
|----|----------|-----------------|-----------------|------|----------|-------------------------------|
| 4 | 0.911310 | 145.254.160.237 | 65.208.228.223 | HTTP | 533 3372 | GET /download.html HTTP/1.1 |
| 5 | 1.472116 | 65.208.228.223 | 145.254.160.237 | TCP | 54 80 | 80 → 3372 [ACK] Seq=1 Ack=480 |
| 6 | 1.682419 | 65.208.228.223 | 145.254.160.237 | TCP | 1434 80 | 80 → 3372 [ACK] Seq=1 Ack=480 |
| 7 | 1.812606 | 145.254.160.237 | 65.208.228.223 | TCP | 54 3372 | 3372 → 80 [ACK] Seq=480 Ack=1 |
| 8 | 1.812606 | 65.208.228.223 | 145.254.160.237 | TCP | 1434 80 | 80 → 3372 [ACK] Seq=1381 Ack= |
| 9 | 2.012894 | 145.254.160.237 | 65.208.228.223 | TCP | 54 3372 | 3372 → 80 [ACK] Seq=480 Ack=2 |
| 10 | 2.443513 | 65.208.228.223 | 145.254.160.237 | TCP | 1434 80 | 80 → 3372 [ACK] Seq=2761 Ack= |
| 11 | 2.553672 | 65.208.228.223 | 145.254.160.237 | TCP | 1434 80 | 80 → 3372 [PSH, ACK] Seq=4141 |
| 12 | 2.553672 | 145.254.160.237 | 65.208.228.223 | TCP | 54 3372 | 3372 → 80 [ACK] Seq=480 Ack=5 |
| 13 | 2.553672 | 145.254.160.237 | 145.253.2.203 | DNS | 89 | Standard query 0x0023 A pagea |
| 14 | 2.633787 | 65.208.228.223 | 145.254.160.237 | TCP | 1434 80 | 80 → 3372 [ACK] Seq=5521 Ack= |
| 15 | 2.814046 | 145.254.160.237 | 65.208.228.223 | TCP | 54 3372 | 3372 → 80 [ACK] Seq=480 Ack=6 |
| 16 | 2.894161 | 65.208.228.223 | 145.254.160.237 | TCP | 1434 80 | 80 → 3372 [ACK] Seq=6901 Ack= |
| 17 | 2.914190 | 145.253.2.203 | 145.254.160.237 | DNS | 188 | Standard query response 0x002 |
| 18 | 2.984291 | 145.254.160.237 | 216.239.59.99 | HTTP | 775 3371 | GET /pagead/ads?client=ca-pub |

> Frame 4: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits)
> Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
> Internet Protocol Version 4, Src: 145.254.160.237, Dst: 65.208.228.223
> Transmission Control Protocol, Src Port: 3372, Dst Port: 80, Seq: 1, Ack: 1, Len: 479
> Hypertext Transfer Protocol

4層になってる！(最初の行は層ではありません)

各層の役割

```
> Frame 4: 533 bytes on wire (4264 bits), 533  
> Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00)  
> Internet Protocol Version 4, Src: 145.254.168.100  
> Transmission Control Protocol, Src Port: 3344  
> Hypertext Transfer Protocol
```

ネットワークインターフェース層

インターネット層

トランスポート層

アプリケーション層

アプリケーション層

役割：アプリケーションごとの固有の規定

主なプロトコル

HTTP・・・HTML文章や画像、音声、動画などの送受信に用いられる

HTTPS・・・TLS/SSLを使ってHTTPの通信を暗号化したもの

FTP・・・異なるコンピュータ間でファイルを転送する時に用いられる

SSH・・・暗号化された遠隔ログインシステム

各層の役割

```
> Frame 4: 533 bytes on wire (4264 bits), 533  
> Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00)  
> Internet Protocol Version 4, Src: 145.254.168.100  
> Transmission Control Protocol, Src Port: 3306  
> Hypertext Transfer Protocol
```

ネットワークインターフェース層

インターネット層

トランスポート層

アプリケーション層

トランスポート層

役割：ノード間のデータ転送の信頼性を確保

主なプロトコル

TCP・・・コネクション型で、信頼性のあるプロトコル

スピード遅い

UDP・・・コネクションレス型で、信頼性のないプロトコル

スピード速い

各層の役割

```
> Frame 4: 533 bytes on wire (4264 bits), 533
> Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00)
> Internet Protocol Version 4, Src: 145.254.1
> Transmission Control Protocol, Src Port: 33
> Hypertext Transfer Protocol
```

ネットワークインターフェース層

インターネット層

トランスポート層

アプリケーション層

インターネット層

役割：ネットワーク間のエンドツーエンドの通信

主なプロトコル

IPv4・・・ネットワークデバイスを識別するためのプロトコル

32ビットのアドレス空間をもつ

IPv6・・・ネットワークデバイスを識別するためのプロトコル

128ビットのアドレス空間をもつ

ARP・・・IPアドレスからMACアドレスを調べる

各層の役割

```
> Frame 4: 533 bytes on wire (4264 bits), 533  
> Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00)  
> Internet Protocol Version 4, Src: 145.254.168.100  
> Transmission Control Protocol, Src Port: 3344  
> Hypertext Transfer Protocol
```

ネットワークインターフェース層

インターネット層

トランスポート層

アプリケーション層

ネットワークインターフェース層

役割：物理的に接続されたノード間の通信

主なプロトコル

Ethernet(有線LAN)

IEEE802.11(無線LAN)

PPP・・・コンピュータ同士の1対1の通信を行うプロトコル

Q. HTTPの下のプロトコルは？



HTTP
TCP？ UDP？

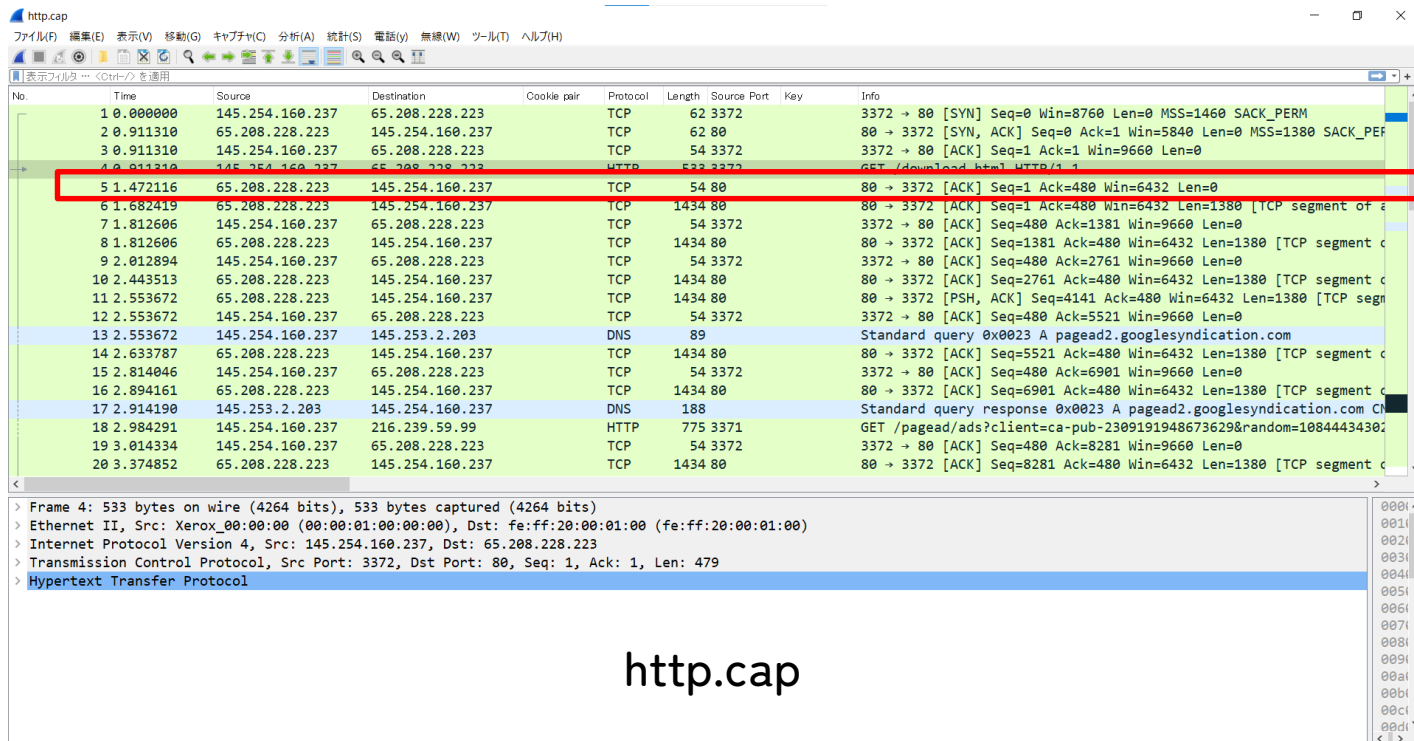
A. TCP

HTTPはWebページを表示するときに使われる
Webページの情報とはデータの漏れなく送りたい

UDPが使われるとWebページを表示する際に、
データが抜け落ちてしまうかも...

TCPパケットの層を確認する

クリック



The image shows a Wireshark packet capture analysis of a file named 'http.cap'. The main packet list pane displays a table of captured packets. Packet 5 is highlighted with a red rectangle, indicating it is the selected packet for detailed analysis.

| No. | Time | Source | Destination | Cookie pair | Protocol | Length | Source Port | Key | Info |
|-----|----------|-----------------|-----------------|-------------|----------|--------|-------------|-----|--|
| 1 | 0.000000 | 145.254.160.237 | 65.208.228.223 | | TCP | 62 | 3372 | | 3372 → 80 [SYN] Seq=0 Win=8760 Len=0 MSS=1460 SACK_PERM |
| 2 | 0.911310 | 65.208.228.223 | 145.254.160.237 | | TCP | 62 | 80 | | 80 → 3372 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM |
| 3 | 0.911310 | 145.254.160.237 | 65.208.228.223 | | TCP | 54 | 3372 | | 3372 → 80 [ACK] Seq=1 Ack=1 Win=9660 Len=0 |
| 4 | 0.911310 | 145.254.160.237 | 65.208.228.223 | | HTTP | 533 | 3372 | | GET /download.html HTTP/1.1 |
| 5 | 1.472116 | 65.208.228.223 | 145.254.160.237 | | TCP | 54 | 80 | | 80 → 3372 [ACK] Seq=1 Ack=480 Win=6432 Len=0 |
| 6 | 1.682419 | 65.208.228.223 | 145.254.160.237 | | TCP | 1434 | 80 | | 80 → 3372 [ACK] Seq=1 Ack=480 Win=6432 Len=1380 [TCP segment of a |
| 7 | 1.812606 | 145.254.160.237 | 65.208.228.223 | | TCP | 54 | 3372 | | 3372 → 80 [ACK] Seq=480 Ack=1381 Win=9660 Len=0 |
| 8 | 1.812606 | 65.208.228.223 | 145.254.160.237 | | TCP | 1434 | 80 | | 80 → 3372 [ACK] Seq=1381 Ack=480 Win=6432 Len=1380 [TCP segment c |
| 9 | 2.012894 | 145.254.160.237 | 65.208.228.223 | | TCP | 54 | 3372 | | 3372 → 80 [ACK] Seq=480 Ack=2761 Win=9660 Len=0 |
| 10 | 2.443513 | 65.208.228.223 | 145.254.160.237 | | TCP | 1434 | 80 | | 80 → 3372 [ACK] Seq=2761 Ack=480 Win=6432 Len=1380 [TCP segment c |
| 11 | 2.553672 | 65.208.228.223 | 145.254.160.237 | | TCP | 1434 | 80 | | 80 → 3372 [PSH, ACK] Seq=4141 Ack=480 Win=6432 Len=1380 [TCP segn |
| 12 | 2.553672 | 145.254.160.237 | 65.208.228.223 | | TCP | 54 | 3372 | | 3372 → 80 [ACK] Seq=480 Ack=5521 Win=9660 Len=0 |
| 13 | 2.553672 | 145.254.160.237 | 145.253.2.203 | | DNS | 89 | | | Standard query 0x0023 A pagead2.googlesyndication.com |
| 14 | 2.633787 | 65.208.228.223 | 145.254.160.237 | | TCP | 1434 | 80 | | 80 → 3372 [ACK] Seq=5521 Ack=480 Win=6432 Len=1380 [TCP segment c |
| 15 | 2.814046 | 145.254.160.237 | 65.208.228.223 | | TCP | 54 | 3372 | | 3372 → 80 [ACK] Seq=480 Ack=6901 Win=9660 Len=0 |
| 16 | 2.894161 | 65.208.228.223 | 145.254.160.237 | | TCP | 1434 | 80 | | 80 → 3372 [ACK] Seq=6901 Ack=480 Win=6432 Len=1380 [TCP segment c |
| 17 | 2.914190 | 145.253.2.203 | 145.254.160.237 | | DNS | 188 | | | Standard query response 0x0023 A pagead2.googlesyndication.com CN |
| 18 | 2.984291 | 145.254.160.237 | 216.239.59.99 | | HTTP | 775 | 3371 | | GET /pagead/ads?client=ca-pub-2309191948673629&random=1084443430 |
| 19 | 3.014334 | 145.254.160.237 | 65.208.228.223 | | TCP | 54 | 3372 | | 3372 → 80 [ACK] Seq=480 Ack=8281 Win=9660 Len=0 |
| 20 | 3.374852 | 65.208.228.223 | 145.254.160.237 | | TCP | 1434 | 80 | | 80 → 3372 [ACK] Seq=8281 Ack=480 Win=6432 Len=1380 [TCP segment c |

The packet details pane for the selected packet (No. 5) shows the following structure:

- Frame 4: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits)
- Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
- Internet Protocol Version 4, Src: 145.254.160.237, Dst: 65.208.228.223
- Transmission Control Protocol, Src Port: 3372, Dst Port: 80, Seq: 1, Ack: 1, Len: 479
- Hypertext Transfer Protocol

http.cap

TCPパケットの層を確認する

| | | | | | |
|----|----------|-----------------|-----------------|------|----------|
| 5 | 1.472116 | 65.208.228.223 | 145.254.160.237 | TCP | 54 80 |
| 6 | 1.682419 | 65.208.228.223 | 145.254.160.237 | TCP | 1434 80 |
| 7 | 1.812606 | 145.254.160.237 | 65.208.228.223 | TCP | 54 3372 |
| 8 | 1.812606 | 65.208.228.223 | 145.254.160.237 | TCP | 1434 80 |
| 9 | 2.012894 | 145.254.160.237 | 65.208.228.223 | TCP | 54 3372 |
| 10 | 2.443513 | 65.208.228.223 | 145.254.160.237 | TCP | 1434 80 |
| 11 | 2.553672 | 65.208.228.223 | 145.254.160.237 | TCP | 1434 80 |
| 12 | 2.553672 | 145.254.160.237 | 65.208.228.223 | TCP | 54 3372 |
| 13 | 2.553672 | 145.254.160.237 | 145.253.2.203 | DNS | 89 |
| 14 | 2.633787 | 65.208.228.223 | 145.254.160.237 | TCP | 1434 80 |
| 15 | 2.814046 | 145.254.160.237 | 65.208.228.223 | TCP | 54 3372 |
| 16 | 2.894161 | 65.208.228.223 | 145.254.160.237 | TCP | 1434 80 |
| 17 | 2.914190 | 145.253.2.203 | 145.254.160.237 | DNS | 188 |
| 18 | 2.984291 | 145.254.160.237 | 216.239.59.99 | HTTP | 775 3371 |

<

> Frame 5: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)

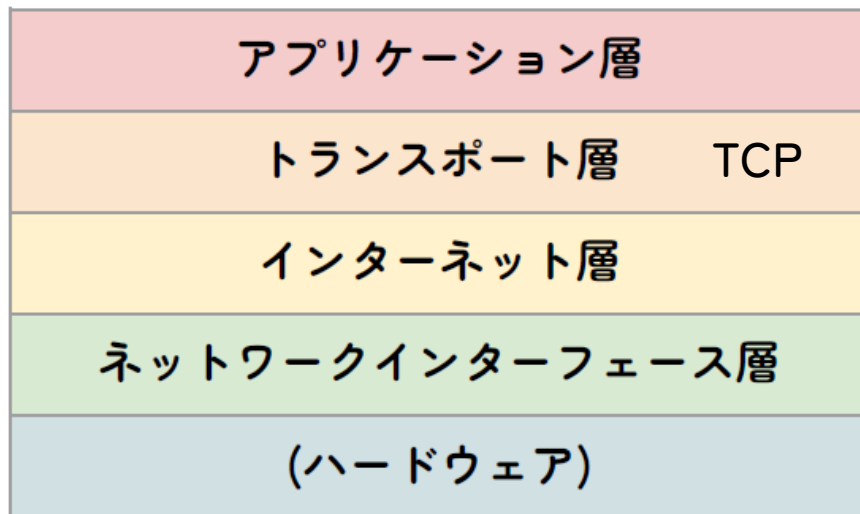
> Ethernet II, Src: fe:ff:20:00:01:00 (fe:ff:20:00:01:00), Dst: Xerox_00:00:00 (00:00:01:00:00:00)

> Internet Protocol Version 4, Src: 65.208.228.223, Dst: 145.254.160.237

> Transmission Control Protocol, Src Port: 80, Dst Port: 3372, Seq: 1, Ack: 480, Len: 0

3層になっている

TCPパケットの層を確認する



ここから通信が始まった

TCPはどうやって信頼性を確保しているのか

—HTTP通信を行う前に何かやりとりしてる？

http.cap

ファイル(F) 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(T) ヘルプ(H)

表示フィルタ: <Ctrl+F> を適用

| No. | Time | Source | Destination | Cookie pair | Protocol | Length | Source Port | Key | Info |
|-----|----------|-----------------|-----------------|-------------|----------|--------|-------------|-----|--|
| 1 | 0.000000 | 145.254.160.237 | 65.208.228.223 | | TCP | 62 | 3372 | | 3372 → 80 [SYN] Seq=0 Win=8760 Len=0 MSS=1460 SACK_PERM |
| 2 | 0.911310 | 65.208.228.223 | 145.254.160.237 | | TCP | 62 | 80 | | 80 → 3372 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM |
| 3 | 0.911310 | 145.254.160.237 | 65.208.228.223 | | TCP | 54 | 3372 | | 3372 → 80 [ACK] Seq=1 Ack=1 Win=9660 Len=0 |
| 4 | 0.911310 | 145.254.160.237 | 65.208.228.223 | | HTTP | 533 | 3372 | | GET /download.html HTTP/1.1 |
| 5 | 1.472116 | 65.208.228.223 | 145.254.160.237 | | TCP | 54 | 80 | | 80 → 3372 [ACK] Seq=1 Ack=480 Win=6432 Len=0 |
| 6 | 1.682419 | 65.208.228.223 | 145.254.160.237 | | TCP | 1434 | 80 | | 80 → 3372 [ACK] Seq=1 Ack=480 Win=6432 Len=1380 [TCP segment of a |
| 7 | 1.812606 | 145.254.160.237 | 65.208.228.223 | | TCP | 54 | 3372 | | 3372 → 80 [ACK] Seq=480 Ack=1381 Win=9660 Len=0 |
| 8 | 1.812606 | 65.208.228.223 | 145.254.160.237 | | TCP | 1434 | 80 | | 80 → 3372 [ACK] Seq=1381 Ack=480 Win=6432 Len=1380 [TCP segment c |
| 9 | 2.012894 | 145.254.160.237 | 65.208.228.223 | | TCP | 54 | 3372 | | 3372 → 80 [ACK] Seq=480 Ack=2761 Win=9660 Len=0 |
| 10 | 2.443513 | 65.208.228.223 | 145.254.160.237 | | TCP | 1434 | 80 | | 80 → 3372 [ACK] Seq=2761 Ack=480 Win=6432 Len=1380 [TCP segment c |
| 11 | 2.553672 | 65.208.228.223 | 145.254.160.237 | | TCP | 1434 | 80 | | 80 → 3372 [PSH, ACK] Seq=4141 Ack=480 Win=6432 Len=1380 [TCP segm |
| 12 | 2.553672 | 145.254.160.237 | 65.208.228.223 | | TCP | 54 | 3372 | | 3372 → 80 [ACK] Seq=480 Ack=5521 Win=9660 Len=0 |
| 13 | 2.553672 | 145.254.160.237 | 145.253.2.203 | | DNS | 89 | | | Standard query 0x0023 A pagead2.google syndication.com |
| 14 | 2.633787 | 65.208.228.223 | 145.254.160.237 | | TCP | 1434 | 80 | | 80 → 3372 [ACK] Seq=5521 Ack=480 Win=6432 Len=1380 [TCP segment c |
| 15 | 2.814046 | 145.254.160.237 | 65.208.228.223 | | TCP | 54 | 3372 | | 3372 → 80 [ACK] Seq=480 Ack=6901 Win=9660 Len=0 |
| 16 | 2.894161 | 65.208.228.223 | 145.254.160.237 | | TCP | 1434 | 80 | | 80 → 3372 [ACK] Seq=6901 Ack=480 Win=6432 Len=1380 [TCP segment c |
| 17 | 2.914190 | 145.253.2.203 | 145.254.160.237 | | DNS | 188 | | | Standard query response 0x0023 A pagead2.google syndication.com CN |
| 18 | 2.984291 | 145.254.160.237 | 216.239.59.99 | | HTTP | 775 | 3371 | | GET /pagead/ads?client=ca-pub-2309191948673629&random=10844434302 |
| 19 | 3.014334 | 145.254.160.237 | 65.208.228.223 | | TCP | 54 | 3372 | | 3372 → 80 [ACK] Seq=480 Ack=8281 Win=9660 Len=0 |
| 20 | 3.374852 | 65.208.228.223 | 145.254.160.237 | | TCP | 1434 | 80 | | 80 → 3372 [ACK] Seq=8281 Ack=480 Win=6432 Len=1380 [TCP segment c |

< >

> Frame 4: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits)

> Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)

> Internet Protocol Version 4, Src: 145.254.160.237, Dst: 65.208.228.223

> Transmission Control Protocol, Src Port: 3372, Dst Port: 80, Seq: 1, Ack: 1, Len: 479

> Hypertext Transfer Protocol

0001
0010
0020
0030
0040
0050

3ウェイハンドシェイク

TCPはデータ転送を行う前に
コネクションの確立を行う

このコネクションの確立のことを
3ウェイハンドシェイクという



<https://www.infraexpert.com/study/tcpip9.html>, ネットワークエンジニアとして

3ウェイハンドシェイク

Info

3372 → 80 [SYN] Seq=0 Win=8760 Len=0 MSS=1460 SACK_PERM

80 → 3372 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM

3372 → 80 [ACK] Seq=1 Ack=1 Win=9660 Len=0

※パケットを追跡する(TCP)

無線(W) ツール(T) ヘルプ(H)

| Destination | Cookie pair | Protocol | Length | Source Port | Key | Info |
|-----------------|-------------|----------|--------|-------------|-----|-----------|
| 65.208.228.223 | | | 62 | 3372 | | 3372 → 80 |
| 145.254.160.237 | | | 62 | 80 | | 80 → 3372 |
| 65.208.228.223 | | | 54 | 3372 | | 3372 → 80 |
| 65.208.228.223 | | | 533 | 3372 | | GET /down |
| 145.254.160.237 | | | 54 | 80 | | 80 → 3372 |
| 145.254.160.237 | | | 434 | 80 | | 80 → 3372 |
| 65.208.228.223 | | | 54 | 3372 | | 3372 → 80 |
| 145.254.160.237 | | | 434 | 80 | | 80 → 3372 |
| 65.208.228.223 | | | 54 | 3372 | | 3372 → 80 |
| 145.254.160.237 | | | 434 | 80 | | 80 → 3372 |
| 145.254.160.237 | | | 434 | 80 | | 80 → 3372 |
| 145.254.160.237 | | | 434 | 80 | | 80 → 3372 |
| 65.208.228.223 | | | 3372 | 80 | | 3372 → 80 |
| 145.253.2.203 | | | | | | Standard |
| 145.254.160.237 | | | | | | 80 → 3372 |
| 65.208.228.223 | | | | | | 3372 → 80 |
| 145.254.160.237 | | | | | | 80 → 3372 |
| 145.254.160.237 | | | | | | Standard |
| 216.239.59.99 | | HTTP | | | | GET /page |
| 65.208.228.223 | | TCP | | | | 3372 → 80 |
| 145.254.160.237 | | TCP | 1434 | 80 | | 80 → 3372 |
| 145.254.160.237 | | TCP | 1434 | 80 | | 80 → 3372 |

追跡したいパケットを右クリック

「追跡」->「TCPストリーム」

プロトコルの話は
キリがないのでここでおわり

この辺が気になる人は マスタリングTCP/IPがオススメ

TCP/IP

マスタリング
TCP/IP

入門編 第6版

井上直也・村山公保・竹下隆史
荒井 透・刈田幸雄 共著



情報工の2年後期でやる
「情報ネットワーク」の教科書

<https://www.ohmsha.co.jp/book/9784274224478/>

CTFにチャレンジ！

CTFとは？

Capture The Flagの略

専門知識や技術を用いて隠されている
Flag(答え)を見つけ出し、点数を競う

CTFとは？

日本ではSECCONが有名

SECCON CTF 2023

| | 日程 Date | 開催イベント Event | 会場 Venue | 内容 Content |
|---|-------------------------|--|------------------------------------|-----------------------------|
| 1 | 2023年9月16日-17日(仮) | SECCON CTF 2023 Quals (SECCON CTF 2023 予選) | オンライン | CTF予選 (日本語 + 英語) |
| 2 | 2023年12月23日(土) -24日 (日) | SECCON CTF 2023 Finals (SECCON 2023 CTF 決勝戦) | 東京 (浅草橋ヒューリックホール & ヒューリック カンファレンス) | 国際CTF大会 (2日間) 国内CTF大会 (2日間) |

<https://www.seccon.jp/2023/seccon/schedule.html>

CTFとは？

世界ではDEFCONが有名

世界最高峰のハッカーが
集まる



The image is a promotional poster for DEFCON 31 CTF Quals. It features a dark background with a stylized, isometric illustration of a cityscape or server racks in shades of blue and green. The text is primarily in white and yellow. At the top left, 'DEFCON' is written in large, blocky, isometric letters. Below it, the dates 'Aug. 10-13, 2023' are displayed. Further down, the location 'Caesars Forum + Flamingo, Harrah's and Linq hotels in Las Vegas, NV' is listed. On the right side, the word 'NEWS' is in green, followed by 'DEF CON 31 CTF Quals Results!' in large white letters. Below this, it says 'Posted 5.30.23'. At the bottom right, there is a quote: 'Just in time to wreck your productivity for the short week, here's some delicious postgame info about the DEF CON 31 CTF Quals that'. In the bottom left corner, there is a small orange square logo with a white '1' inside.

DEFCON

Aug. 10-13, 2023

Caesars Forum + Flamingo,
Harrah's and Linq hotels
in Las Vegas, NV

NEWS

**DEF CON 31 CTF Quals
Results!**

Posted 5.30.23

**CTF QUALS
2023**

Just in time to wreck your
productivity for the short week,
here's some delicious
postgame info about the DEF
CON 31 CTF Quals that

<https://defcon.org/html/defcon-31/dc-31-index.html>

問題ダウンロード

<https://onedrive.live.com/?authkey=%21ANE0wqC%5Ftrouhy0&id=5EC2715BAF0C5F2B%2110056&cid=5EC2715BAF0C5F2B>

ctf4b



名前 ↑ ↓

更新日時 ↓

ファイル サイズ ↓

共有



ctf4b_講義_binary.zip

2022/5/31

10.2 MB

共有



ctf4b_講義_network.zip

2022/5/31

5.82 MB

共有