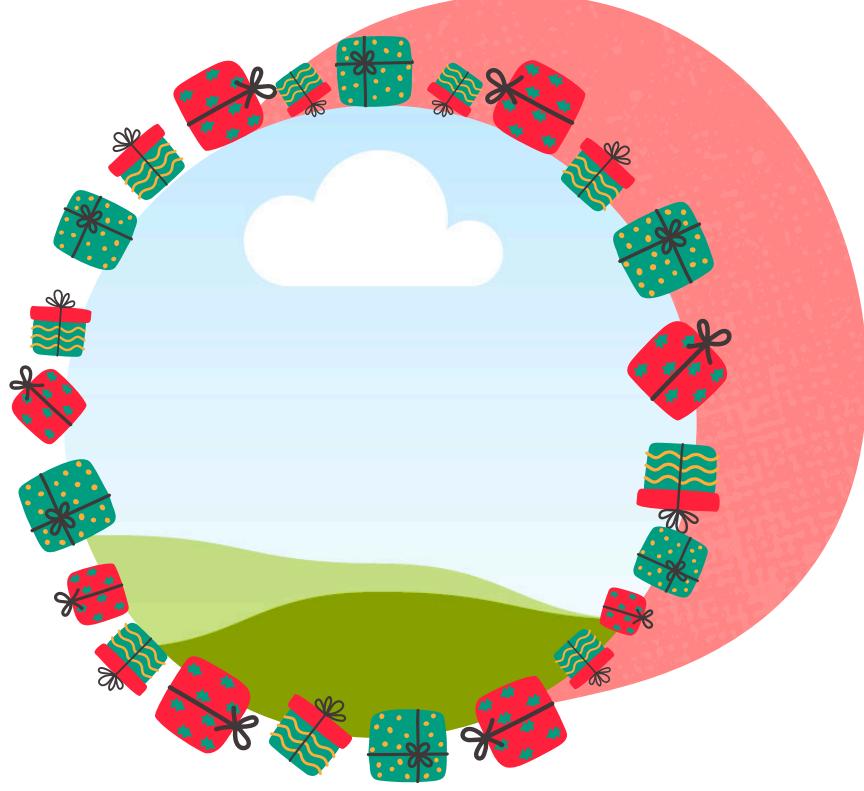




# 情報セキュリティ

# アッププロジェクト



R6.12.25 CTF\_Network

工学部情報工学科3年 大城優賀



# 今日の流れ

Netwokについて

知識の復習&勉強

ツールの紹介

ツール使い方

Network問題&解説

# Networkについて





Network  
について

CTFにおけるNetworkとは  
パケットキャプチャやプロトコ  
ル解析などの手法をもちいて  
ファイル内の「FLAG」を見つ  
け出す。

# Network について

問題を解くうえで求められる  
ポイントは通信がどのようにして  
可能になっているか理解すること。

# Network について

CTFのNetwork問題を解くう  
えで、特にOSI参照モデルの第3  
層、第4層、第7層の各プロト  
コルについて理解を深める。

# 必要な知識の 復習 & 勉強



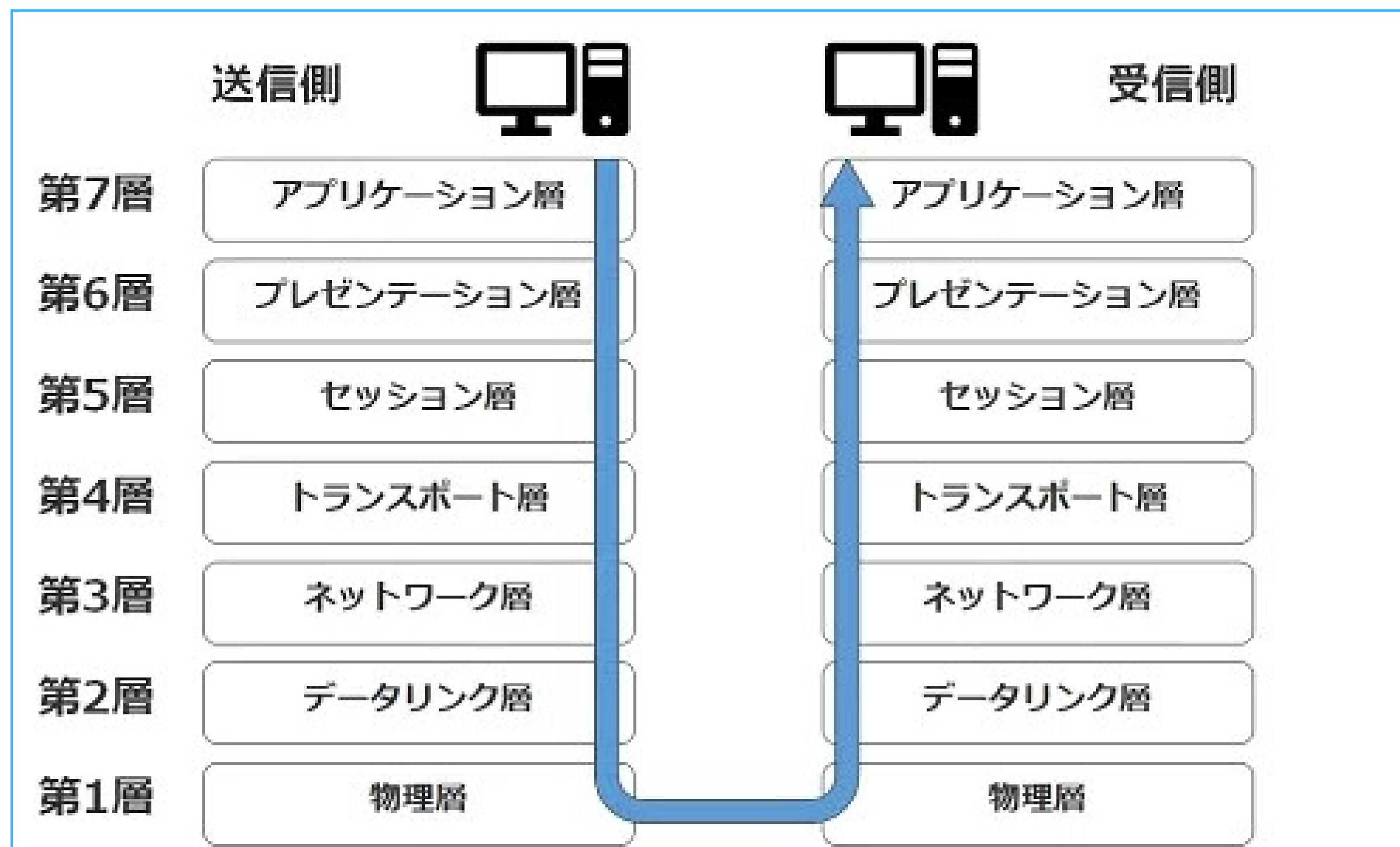
# どのように通信しているのか

## OSI参照モデル

L	層名	定義	プロトコル例
L7	アプリケーション層	アプリケーション、サービス	HTTP, FTP, 電子メール
L6	プレゼンテーション層	データの表現形式	文字コード、圧縮
L5	セッション層	接続制御と管理	TLS
L4	トランSPORT層	データ通信の制御	TCP/IP, UDP
L3	ネットワーク層	アドレス管理とルーティング	IPv4, IPv6
L2	データリンク層	通信区間のデータ送受信	Ethernet, Wi-Fi
L1	物理層	電気信号、無線信号	有線ケーブル、無線

# どのように通信しているのか

## データ送受信の流れ



# 重視するレイヤー（層）

## OSI参照モデル

L	層名	定義	プロトコル例
L7	アプリケーション層	アプリケーション、サービス	HTTP, FTP, 電子メール
L6	プレゼンテーション層	データの表現形式	文字コード、圧縮
L5	セッション層	接続制御と管理	TLS
L4	トランSPORT層	データ通信の制御	TCP/IP, UDP
L3	ネットワーク層	アドレス管理とルーティング	IPv4, IPv6
L2	データリンク層	通信区間のデータ送受信	Ethernet, Wi-Fi
L1	物理層	電気信号、無線信号	有線ケーブル、無線

# 3層 ネットワーク層

## 役割

ネットワーク層は通信相手を識別するためにIPアドレスの割り当てを行ったり、IPアドレスを元にデータを適切な経路選択を行う。

# 3層 ネットワーク層

## 重要なプロトコル

IP：ホストへデータ送信するため

ARP：IPアドレスからMACアドレスを求める

ICMP：データ転送のエラーを通知する

# 4層 トランスポート層

## 役割

データの送信元と送信先の間での制御や通知、交渉などを行い、二者間のデータ運搬の責任を持つ

# 4層 トランSPORT層

## 重要なプロトコル

UDP：コネクション型。信頼性のあるプロト

コルである。例. 電話

TCP：コネクションレス型。信頼性のないプロトコルである。例. メール

# 7層 アプリケーション層

## 役割

特定の具体的なシステムやサービスに必要な機能を実装する。

アプリケーション間のデータのやり取りを規定する

# 7層 アプリケーション層

## 重要なプロトコル

HTTP : WebサーバとWebブラウザ間のweb

ページのやり取りをする

FTP : サーバとファイルのやり取りをする。

※通信が暗号化されていない。

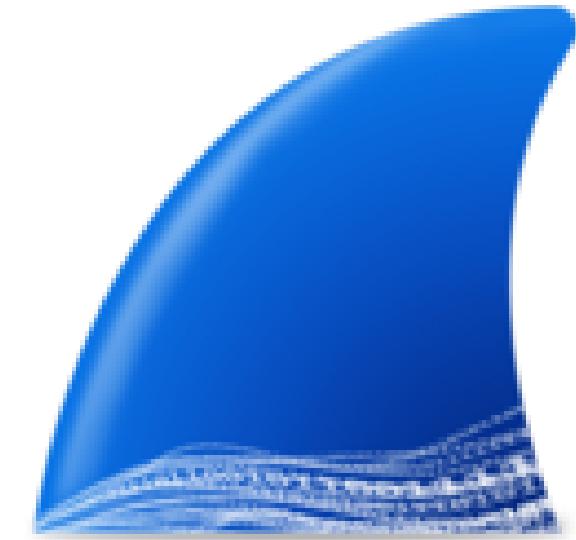
SMTP : 電子メールの送受信する

# ツールの紹介





様々なプロトコルのパケットが  
記録されているpcapファイルを  
解析してファイル内から「Flag」  
を見つける  
これらのファイルをWireshark  
を用いて解析する



# ツールの使い方



## 操作メニュー

表示  
フィルタ

表示フィルタ <Ctrl-/> を適用

No.	Time	Source	Destination	Protocol	Length	Info
49	3.025231	192.168.0.90	142.250.206.194	TCP	55	55601 → 443 [ACK] Seq=1 Ack=1 Win=1020 Len=1 [TCP segment of a reassembly, reassembled 1 segments in total (see reassembly cache)]
50	3.030779	142.250.206.194	192.168.0.90	TCP	66	443 → 55601 [ACK] Seq=1 Ack=2 Win=1036 Len=0 SLE=1 SRE=2
51	3.058871	192.168.0.90	142.250.206.225	TCP	55	55609 → 443 [ACK] Seq=1 Ack=1 Win=1025 Len=1 [TCP segment of a reassembly, reassembled 1 segments in total (see reassembly cache)]
52	3.064914	142.250.206.225	192.168.0.90	TCP	66	443 → 55609 [ACK] Seq=1 Ack=2 Win=1046 Len=0 SLE=1 SRE=2
53	3.067255	192.168.0.90	142.250.206.194	TCP	55	55602 → 443 [ACK] Seq=1 Ack=1 Win=1020 Len=1 [TCP segment of a reassembly, reassembled 1 segments in total (see reassembly cache)]
54	3.072833	142.250.206.194	192.168.0.90	TCP	66	443 → 55602 [ACK] Seq=1 Ack=2 Win=1036 Len=0 SLE=1 SRE=2
55	3.075641	192.168.0.90	142.250.206.225	TCP	55	55605 → 443 [ACK] Seq=1 Ack=1 Win=1024 Len=1 [TCP segment of a reassembly, reassembled 1 segments in total (see reassembly cache)]
56	3.081393	142.250.206.225	192.168.0.90	TCP	66	443 → 55605 [ACK] Seq=1 Ack=2 Win=1045 Len=0 SLE=1 SRE=2
57	3.092040	192.168.0.90	172.217.25.170	TCP	55	55603 → 443 [ACK] Seq=1 Ack=1 Win=1024 Len=1 [TCP segment of a reassembly, reassembled 1 segments in total (see reassembly cache)]
58	3.097475	172.217.25.170	192.168.0.90	TCP	66	443 → 55603 [ACK] Seq=1 Ack=2 Win=1046 Len=0 SLE=1 SRE=2
59	3.116683	192.168.0.90	142.250.206.194	TCP	55	55610 → 443 [ACK] Seq=1 Ack=1 Win=1020 Len=1 [TCP segment of a reassembly, reassembled 1 segments in total (see reassembly cache)]
60	3.122484	142.250.206.194	192.168.0.90	TCP	66	443 → 55610 [ACK] Seq=1 Ack=2 Win=1040 Len=0 SLE=1 SRE=2
61	3.200030	192.168.0.90	142.250.206.194	TCP	55	55614 → 443 [ACK] Seq=1 Ack=1 Win=1025 Len=1 [TCP segment of a reassembly, reassembled 1 segments in total (see reassembly cache)]
62	3.200099	192.168.0.90	142.250.76.131	TCP	55	55615 → 443 [ACK] Seq=1 Ack=1 Win=1025 Len=1 [TCP segment of a reassembly, reassembled 1 segments in total (see reassembly cache)]
63	3.205725	142.250.76.131	192.168.0.90	TCP	66	443 → 55615 [ACK] Seq=1 Ack=2 Win=1047 Len=0 SLE=1 SRE=2
64	3.205731	142.250.206.194	192.168.0.90	TCP	66	443 → 55614 [ACK] Seq=1 Ack=2 Win=1043 Len=0 SLE=1 SRE=2
65	3.309443	192.168.0.90	172.67.75.39	TCP	55	55362 → 443 [ACK] Seq=1 Ack=1 Win=1028 Len=1 [TCP segment of a reassembly, reassembled 1 segments in total (see reassembly cache)]
66	3.320475	172.67.75.39	192.168.0.90	TCP	65	443 → 55362 [ACK] Seq=1 Ack=2 Win=9 Len=0 SLE=1 SRE=2
67	3.366819	192.168.0.90	172.67.75.39	TCP	55	55361 → 443 [ACK] Seq=1 Ack=1 Win=1024 Len=1 [TCP segment of a reassembly, reassembled 1 segments in total (see reassembly cache)]
68	3.377508	172.67.75.39	192.168.0.90	TCP	66	443 → 55361 [ACK] Seq=1 Ack=2 Win=10 Len=0 SLE=1 SRE=2
69	3.384694	57.182.116.188	192.168.0.90	TLSv1.2	93	Application Data

Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0  
 Ethernet II, Src: ToshibaClient\_88:2c:40 (68:45:f1:88:2c:40), Dst: 192.168.0.90 (08:00:27:00:00:90)  
 Internet Protocol Version 4, Src: 192.168.0.90, Dst: 202.138.10.1 (80:0c:90:00:00:90)  
 Transmission Control Protocol, Src Port: 55666, Dst Port: 80 (HTTP)

0000 f0 09 0d 77 8c 14 68 45 f1 88 2c 40 08 00 45 00 ..w..hE ..,@..E.  
 0010 00 34 87 cc 40 00 80 06 47 bb c0 a8 00 5a ca 0d ..4..@..G..Z..  
 0020 a0 2c d9 72 1f 90 d9 02 28 c9 00 00 00 00 80 02 ..,r...((.....  
 0030 fa f0 4e 14 00 00 02 04 05 b4 01 03 03 08 01 01 ..N.....  
 0040 04 02 ..

23 バイ (Protocol (p.proto))

パケット数: 813 表示: 813 (100.0%) 欠落: 0 (0.0%) プロファイル: Default

# Network

## 例題と解説



slack にあげた  
フォルダをダウンロード  
してください

Flag形式は以下の通り

kitCTF{xxxxxxxx}



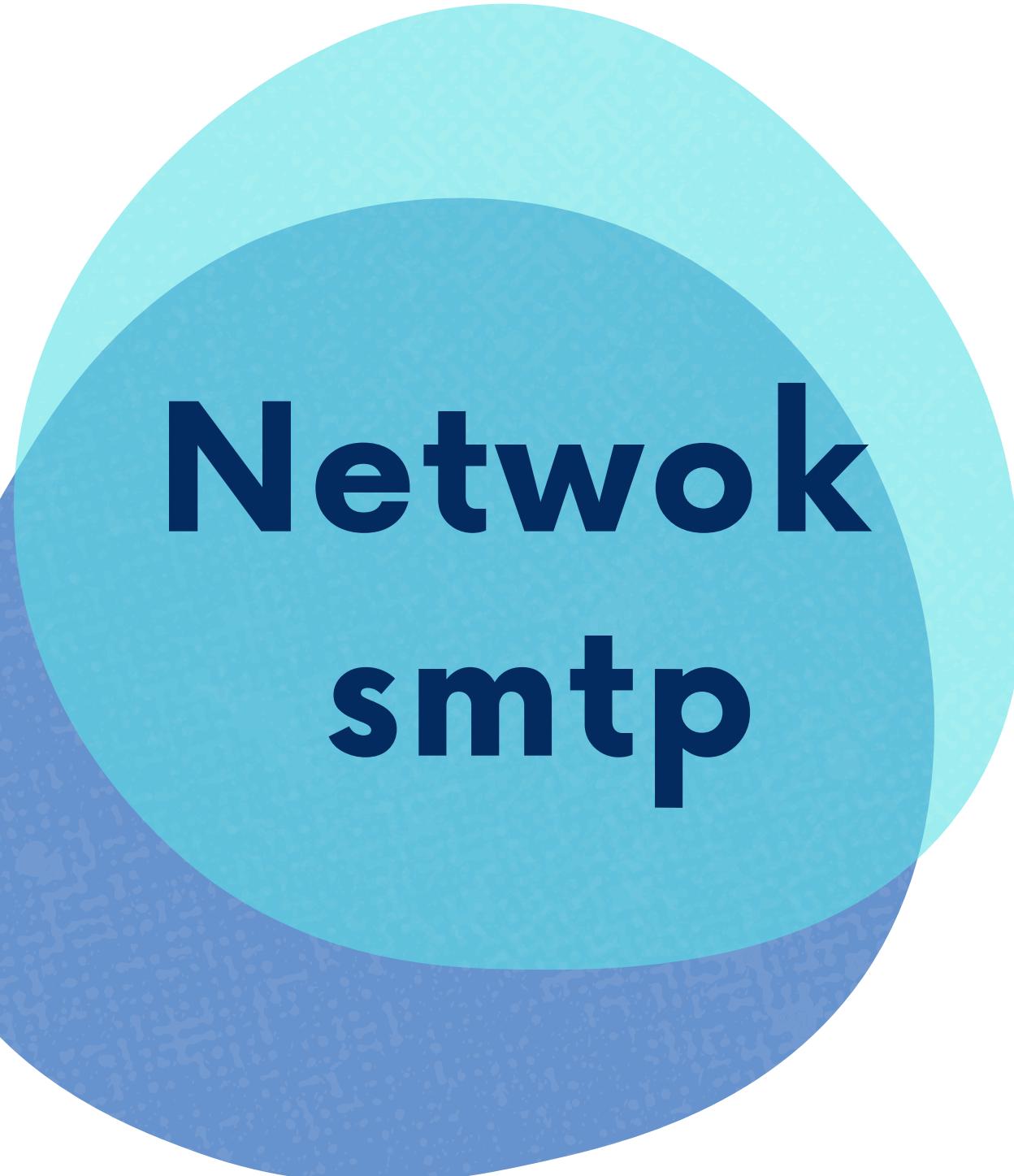
Netwok  
http

パケット表示エリアを  
眺めてください。  
どのような通信をしているのか  
考えながら「Flag」を  
探してください。

# ヒント

「http」に注目すると、  
このファイルはweb通信をしていると  
考えられる。

「http」パケットの「Info」に注目する  
ことで、「Flag」の手がかりがある



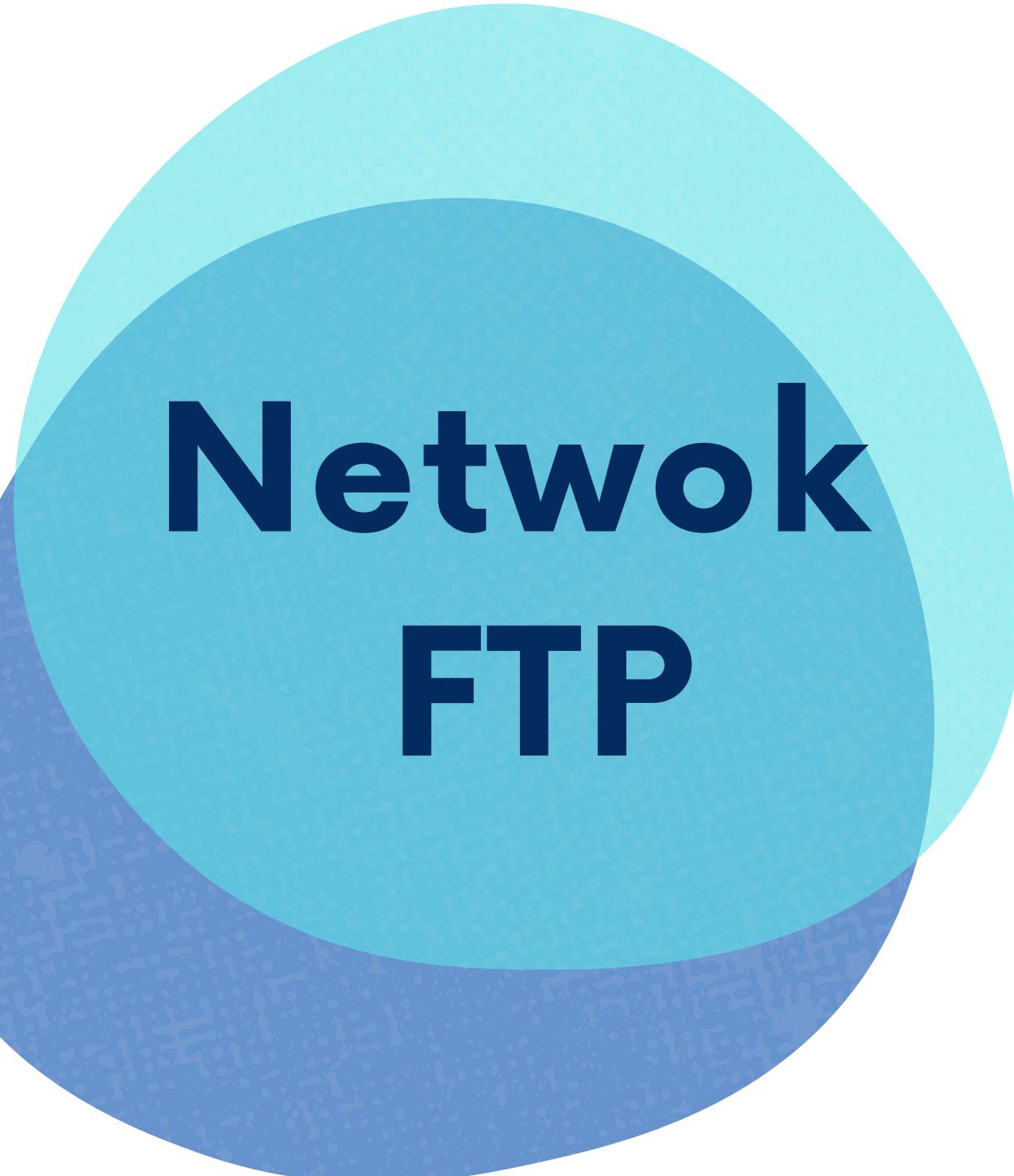
Netwok  
smtp

smtpを使ったメール送信を  
行いました。  
ファイルを解析し、「Flag」を  
見つけてください。

# ヒント

「smtp」を使ったメール送信を行っている。

「TCPストリーム」をすることで、メール内容が見れる。



Netwok  
FTP

あなたは「FTP」を使った  
ファイルの送受信を行っている  
パケットファイル入手した。  
これを解析して、「Flag」を  
見つけてください

# ヒント

「FTP」は通信経路が暗号化されていない

「ftp」関連に「Flag」がありそう

「ftp」は制御用チャンネル

「ftp-data」はデータ転送用チャンネル

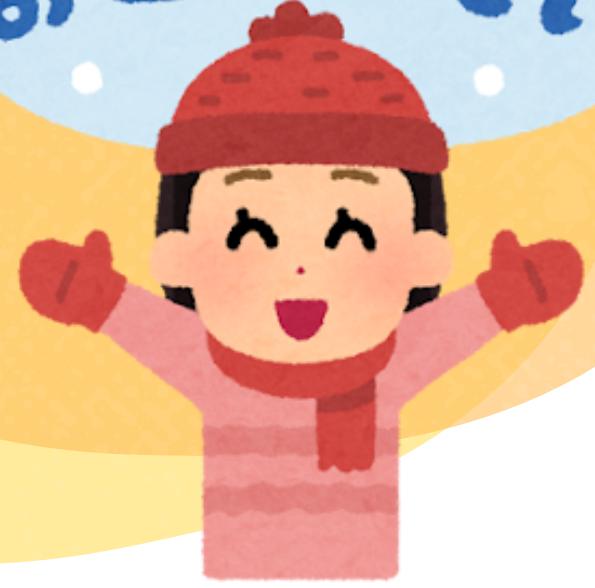
「ftp-data」が怪しい？

今年お疲れ様でした！  
来年もよろしくお願  
い  
します！！

良いお年を  
お迎え下さい



良いお年を  
お迎え下さい



良いお年を！！

