情報工学実験 III　実験⑤ ネットワークプロトコル

第 1 回 Windows プラットフォーム上での実験 【Rel. 20190315A】

目的

TCP/IP プロトコルと、関連する各種上位プロトコルの基礎を学ぶ。具体的には、各プロトコルを実装したコマンド（アプリケーション プログラム）を実行し、各プロトコルの機能等を確認する。また、同じプロトコルを実装したコンピュータ間では、OS プラットフォームに関係なく通信が行えることを確認する。

0. 実験環境の準備
- 個人用ファイル格納フォルダの作成 -

Windows にログオンし、デスクトップ上の「jikkenuser」フォルダ内に、新たにフォルダを作成する。フォルダの名前は、s12a3456 のように s+学籍番号とし、実験室 PC 上に個人用ファイルを作成する場合は、このフォルダに格納する。

1. コンピュータのネットワーク関連情報を調査する
- ipconfig コマンド -

Windows プラットフォーム上でネットワーク関連情報を調査するには、ipconfig コマンドを用いる。このコマンドで自コンピュータ（自ホスト）の IP アドレス等、多くの情報を得ることができる。

◆実験　自席パソコンの有線 LAN ネットワーク（イーサネット）関連情報を調べる。

【手順 1】コマンドプロンプトを起動する。（ ⊞+R キーを押下し、『ファイル名を指定して実行』画面を表示→名前(O):欄に『cmd』と入力→OK をクリック）

【手順 2】コマンドプロンプト画面に 『ipconfig　/all』と入力

▼ 出力された内容のうち、「イーサネット アダプター イーサネット：」の部分を記録し、これを【レポート 1】とする。

可能であれば、表示された各項目の意味を調べ、説明せよ（オプション）。

※注　　特に"IPv4 アドレス"の値に注意する。この値が自ホストの IP アドレスとなる。
（後の実験で、この情報「自ホストの IP アドレス」が必要になる。）

2. ホスト名と IP アドレスを調査する
- DNS: Domain Name System -

通常、私たちが Web ブラウザ上から各種サイトを指定する際には、www.fit.ac.jp 等の英数字からなるホスト名を使用するが、実際に自コンピュータが、あるサイトのコンピュータ（サーバ）と通信するには、IP アドレスを知る必要がある。ここで、ホスト名←→IP アドレス間の変換を行う仕組みが DNS(Domain Name System)である。私たちが、ホスト名を用いて相手コンピュータを指定した場合でも、多くの場合はプログラム内部で自動的に、DNS による変換が行われ、実際には IP アドレスを使用した通信が行われる。

ここでは、DNS プロトコルを利用するプログラムの例として、nslookup コマンドを使用し、DNS サーバへの問い合わせを手動で行う。nslookup コマンドは、ユーザがコマンドで指定したコンピュータ（サイト）のホスト名と IP アドレスの対応を、DNS サーバと通信して調査し、ユーザに回答する（DNS サーバに関する情報も同時に得られる）。

```
C:¥Users¥jikkenuser> nslookup www.fit.ac.jp

サーバー:  ad01.bene.fit.ac.jp   …【DNS サーバのホスト名】
Address:  150.43.169.30          …【DNS サーバの IP アドレス】

権限のない回答:
名前:    fitweb.ipc.fit.ac.jp    …【ホスト名(本名)】
Address:  150.43.1.10            …【IP アドレス】
Aliases:  www.fit.ac.jp          …【ホスト名(別名)】
```

問い合わせに対して回答した DNS サーバに関する情報 ※今回は不要(参考)

問い合わせに対する回答情報（www.fit.ac.jp の IP アドレスの他、www.fit.ac.jp は別名で、本名は fitweb.ipc.fit.ac.jp であることを表している）

図 1　ホスト名『www.fit.ac.jp』を DNS サーバに問い合わせた場合の例

◆実験　次表のコンピュータのホスト名・IP アドレスを調査し、表 1 を完成させる。

【手順】　コマンドプロンプトに『nslookup **www.abc.jp**』や『nslookup **123.45.67.89**』の形式で入力し、対応する IP アドレスやホスト名を調べる。
▼ 結果を記録し、完成した表 1 全体を【レポート 2】とする。

※注 1　DNS サーバへ問い合わせた結果、複数のホスト名／IP アドレスが返却されることがある。このような場合、表には最初に現れたホスト名／IP アドレスを記入する（すべて記入しても良い）。

※注 2　nslookup コマンドで xyz を問い合わせた結果、「＊＊＊（DNS サーバ）が xyz を見つけられません: (理由コード）」などのエラーが返ってくることがある。これは、DNS データベース上に、ホスト名あるいは IP アドレスが登録されていない等の理由による。このような場合、表には「<不明>」と記入すること。

表 1　ホスト名と IP アドレスの対応

	コンピュータの種類	ホスト名（本名）	IP アドレス
【例】	福工大 Web サイト	(fitweb.ipc.fit.ac.jp)	150.43.1.10
	情報基盤センターサーバ	ipcs.bene.fit.ac.jp	
	実験室内プリンタ(PR1)		150.43.61.77
	実験室内プリンタ(PR2)		150.43.61.78
	実験室内プリンタ(PR3)		150.43.61.79
	朝日新聞社 Web サイト	www.asahi.com	
	自席パソコン		
	(任意のサイト 1)		
	(任意のサイト 2)		
	(任意のサイト 3)		

3. 通信相手からの応答があるかどうかを調査する
- ICMP: Internet Control Message Protocol -

IP プロトコルのレベルで、通信できるかどうかを確認するために、ping コマンドがよく使用される。ping コマンドは、通信相手にパケットを送信し、相手からの応答を要求する。ネットワークアプリケーションで通信が正常に行えない場合、まず、ping コマンドで通信相手からの応答があるかどうかを調べることにより、問題を初期段階で切り分けることができる。例えば、あるサイトについて ping による応答がない場合、IP プロトコルレベルでの通信が失敗しており、例えばそのサイト自身がダウンしている可能性があると考えられる。また、ping による応答があるにもかかわらず、ネットワークアプリケーションの通信が正常に行えない場合は、アプリケーションが使用するプロトコルレベルでの問題が生じていることが考えられる。なお、ping コマンドは、ICMP プロトコル(Internet Control Message Protocol)を利用している。下図に、ping コマンドの実行例を示す。

```
C:¥Users¥jikkenuser> ping xxx.ac.jp

xxx.ac.jp [nn.nn.nn.nn]に ping を送信しています 32 バイトのデータ:

nn.nn.nn.nn からの応答: バイト数 =32 時間 =3ms TTL=250
        :    【↑ 相手からの応答がある場合は、応答に要した時間等が表示される】
        :
(mm.mm.mm.mm からの応答: 宛先ホストに到達できません。)
        :    【↑ 相手からの応答がない場合は、ルータ等からのエラーが表示される】
        :
【デフォルトでは、ping パケットを 4 回送信した結果を表示した後、統計情報が表示される。】
```

図 2　ホスト名『xxx.ac.jp』に対して ping コマンドを実行した場合の例

◆実験　次表のコンピュータに対し、ping コマンドを実行し、表 2 を完成させる。

【手順】　コマンドプロンプトに、『ping **www.abc.jp**』または『ping **123.45.67.89**』の形式で入力し、応答の有無を調べる。

▼ 結果を記録し、完成した表 2 全体を【レポート 3】とする。

表 2　ping コマンドを使用した応答あり/なしの調査

コンピュータの種類	ホスト名または IP アドレス	応答あり/なし
myFIT サイト	my.fit.ac.jp	
情報基盤センターサーバ	ipcs.bene.fit.ac.jp	
実験室内プリンタ(PR1)	150.43.61.77	
実験室内プリンタ(PR2)	150.43.61.78	
実験室内プリンタ(PR3)	150.43.61.79	
朝日新聞社 Web サイト	www.asahi.com	
実験室パソコン(教員席)	150.43.61. [　] ←当日発表	
不明なアドレス	150.43.248.42	
(任意のサイト 1)		
(任意のサイト 2)		

（「あり」か「なし」だけの記入で OK ）

ping コマンドで使用される ICMP プロトコル（ICMP echo パケット）は、ファイアウォール・ルータ類によって遮断する設定にされることが多くなってきている。したがって、ping コマンドの応答がない場合、本当に相手ホストが応答していない場合だけでなく、経路上で遮断されている可能性も考慮しなければならない。

4. IP アドレスを動的に取得する
- DHCP: Dynamic Host Configuration Protocol -

インターネット黎明期は、コンピュータの IP アドレス等の設定は、手作業で行っていたが、DHCP(Dynamic Host Configuration Protocol)の普及により、現在ではネットワーク関連の情報は DHCP サーバから取得できるようになり、自動的に設定されるようになった。この DHCP では、パソコンをはじめとする DHCP クライアント機は、ネットワーク設定を一括管理する DHCP サーバに対して問い合わせを行う。その後、サーバにより提供された、そのネットワークに適した IP アドレスやサブネットマスク等の設定情報を用いてクライアント機の設定を行う。

Windows プラットフォーム上で DHCP 関連の操作を行うには前出の ipconfig コマンドの /release オプションや /renew オプションを用いる。

◆実験　自席パソコンの IP アドレスをいったん解放し、再度 DHCP サーバから割り当てを受ける（実験室のパソコンは、起動時に DHCP により IP アドレスの割り当てを既に受けている。そこでこのアドレスをいったん解放した上で、再度 IP アドレスの取得を試みる）。

【手順 1】既に割り当てを受けている IP アドレスを解放する。
コマンドプロンプト画面に『ipconfig　/release』と入力する。
▼出力された内容のうち、「イーサネット アダプター イーサネット：」の部分に IPv4 アドレス欄が表示**されない**ことを確認する。

【手順 2】DHCP サーバより、IP アドレスの割り当てを受ける。
コマンドプロンプト画面に『ipconfig　/renew』と入力
▼ IPv4 アドレスが 150.43.61.xx と表示されることを確認する。

【手順 3】DHCP サーバより IP アドレスの割り当てを受けた時刻を確認する。
コマンドプロンプト画面に『ipconfig　/all』と入力
▼ 「イーサネット アダプター イーサネット：」部の“リース取得”と“リースの有効期限”の 2 行ぶんを記録し、これを【レポート 4】とする。

5. ネットワーク上でやりとりするパケットの内容を解析する
- Wireshark ネットワークプロトコルアナライザ アプリケーション -

ここでは、Wireshark という、フリーのネットワークアナライザプログラムを使用して、自ホストがネットワークに対してやりとりしているパケットの内容を解析する（パケットデータの中から DNS プロトコルのパケットを見つけ、調査する）。

◆Wireshark プログラムの起動
⊞+R キーを押下し、『ファイル名を指定して実行』画面を表示→名前(O):欄に
『wireshark-gtk』と入力→OK をクリックする。
※スタート画面から起動する場合は『Wireshark Legacy』を選ぶ。（従来互換インタフェース版を使用する。）
▼ Wireshark プログラムが起動することを確認する。
※『新しいバージョンの Wireshark がご利用いただけます。』ダイアログが出現した場合、『このバージョンをスキップする』を選んで、実験を続ける。

Wireshark では、プログラム内にパケットを取り込むことを『**キャプチャ**』と呼び、キャプチャを開始してから停止するまでの間、コンピュータ上でやりとりする、すなわち、NIC（ネットワークインタフェースカード）で送受信するパケットをキャプチャし続ける。

◆実験 1　ブラウザで任意の Web サイトを閲覧し、その間に自ホストがやりとりしたパケットを Wireshark でキャプチャする。

【手順 1】キャプチャを開始する。
Wireshark ツールバー左端の『(List the available capture interfaces...)』ボタンを押し、出現した『Wireshark: Capture Interfaces』ダイアログで、Device『イーサネット』チェックされてい

ることを確認し、『Start』ボタンを押す（図 3 参照）。

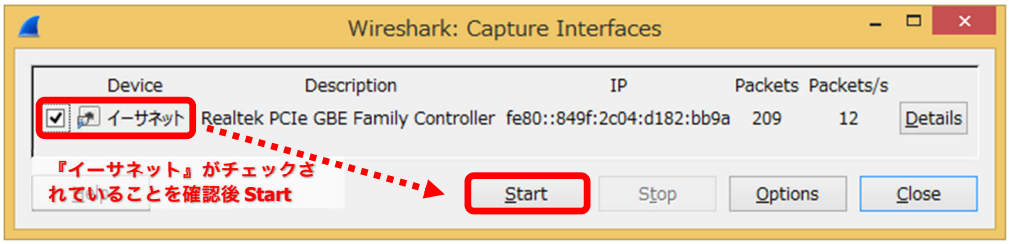


図 3　Wireshark: Capture Interfaces ダイアログ

▼ 同ダイアログが消え、現在送受信中のパケットのキャプチャが開始されたことを確認する（Wireshark のメイン画面上に、キャプチャしたパケットが 1 行ずつリアルタイムに表示されていく）。

【手順 2】Microsoft Edge や Firefox 等のブラウザを起動し、任意の Web サイトを閲覧する。その際、これまでの実験で既にアクセスしたことのあるサイトは避ける。

【手順 3】キャプチャを停止する。

Wireshark ツールバーの左側から 4 番目にある『■(赤い四角形：Stop the running live capture)』ボタンを押す。

Wireshark のメイン画面の例を図 4 に示す。デフォルト状態では、画面は 3 つのペインに分割される。第 1～第 3 ペインはそれぞれ、パケット一覧部・パケット詳細部・パケットデータ部と呼ばれる。

送信あるいは受信した 1 つのパケットは、パケット一覧部内の 1 行に相当する。また、パケット詳細部には、パケット一覧部で選択した（反転させた行の）パケットの詳細な構造（プロトコル毎に異なる各種フィールドの値など）が表示され、またそれと同時に、パケットデータ部には、選択したパケットの実データが 16 進ダンプ＋ASCII 文字表記で表示される。

（※この実験 1 では、レポートに記載する箇所は特にない。キャプチャを行うだけで、次の実験 2 へ進んで良い。）

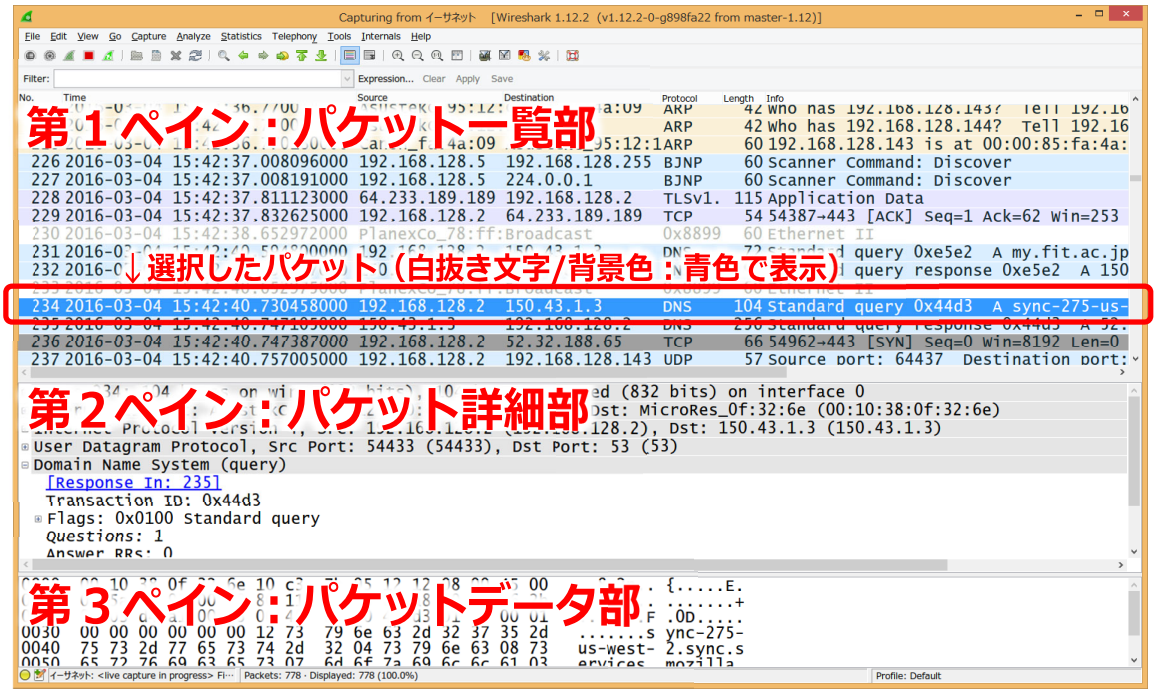


図 4　Wireshark メイン画面の例

◆実験 2　前実験でキャプチャしたデータの中に含まれる、DNS パケットのやりとりの様子を確認する。具体的には、自ホストが DNS サーバへ送信したパケット(query)および、DNS サーバから受信したそのレスポンス（query **response**）パケットの組を 3 組以上見つけ、表 3 を完成させる。

表 3　DNS パケットのやりとりの様子

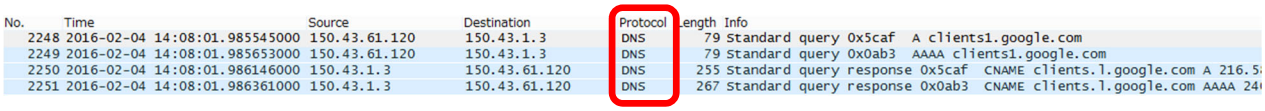
DNS パケットの種類		パケット取得時刻 (Time, 01:02:03.123456 形式)	発信元 IP アドレス (Source)	宛先 IP アドレス (Destination)
1	問い合わせ(query)			
	回答(query response)			
2	問い合わせ (query)			
	回答(query response)			
3	問い合わせ(query)			
	回答(query response)			

【手順】　キャプチャしたデータの中から DNS パケットを見つける。

《前準備》『Time』フィールドの表示形式を 01:02:03.123456 の様な形式に変更する。

（表示形式が、すでにこの形式であれば不要。）この形式になっていない場合は、メニューより『View』-『Time Display Format』-『Time of Day: 01:02:03.123456』を選んで変更する。（または、ショートカットキー『Ctrl+Alt+2』を使用する。）

▼『Protocol』フィールドが『DNS』となっている行（パケット）を見つける。通常、自ホストが送信した問い合わせ(query)の直後に、DNS サーバからの回答／レスポンス(query response)が受信されている。このペアをひと組とする。



No.	Time	Source	Destination	Protocol	Length	Info
2248	2016-02-04 14:08:01.985545000	150.43.61.120	150.43.1.3	DNS	79	Standard query 0x5caf A clients1.google.com
2249	2016-02-04 14:08:01.985653000	150.43.61.120	150.43.1.3	DNS	79	Standard query 0x0ab3 AAAA clients1.google.com
2250	2016-02-04 14:08:01.986146000	150.43.1.3	150.43.61.120	DNS	255	Standard query response 0x5caf CNAME clients.l.google.com A 216.5
2251	2016-02-04 14:08:01.986361000	150.43.1.3	150.43.61.120	DNS	267	Standard query response 0x0ab3 CNAME clients.l.google.com AAAA 24

図 5　DNS パケットの例（この場合 2 組=4 つの DNS パケットが続いている）

ここで、『Info』フィールドが『Standard **query** 0x1abc A xxxxxx』となっている DNS パケットが、自ホストから DNS サーバに対して送信した問い合わせ（query）になる。このパケットは、自ホストから発信したものなので、『Source』（発信元）フィールドが自ホストの IP アドレス、『Destination』（宛先）フィールドのアドレスは、DNS サーバの IP アドレスとなる。また、『Info』フィールドが『Standard query **response** 0x1abc …』で始まる DNS パケットが、 DNS サーバから受信した、回答／レスポンス（query response）であり、『Source』と『Destination』のアドレスが、前述の問い合わせ（query）の逆になっていることがわかる。

※補足　このように、DNS のパケットには、query と response の 2 種類があり、『Info』項目や『Source』と『Destination』アドレスで識別できる。さらに、例の場合では、query A(IPv4 アドレスの問い合わせ)と query AAAA(IPv6 アドレスの問い合わせ)が連続して行われている。

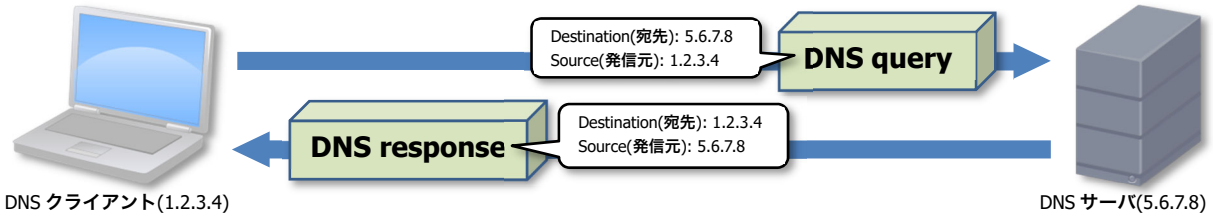


図 6　DNS クライアントとサーバ間でやりとりされるパケット

▼ 結果を記録し、完成した表 3 全体を【レポート 5-1】とする。

▼もし、DNS のパケットが見つからない場合や、query パケットとその回答の query response パケットのペアが揃わない場合、前実験に戻り、再度キャプチャを行う。その際、本日既にアクセスしたことのある Web サイトは避け、本日初めての Web サイトをアクセスすると良い（一度アクセスしたサイトのアドレスは OS のキャッシュに保管され、DNS パケットのやりとりが生じないため）。

次の実験では、パケットの構造の解析を行う。

ネットワーク上でやりとりされるパケットは、通常ヘッダ部とデータ部に分けることができる。たとえばイーサネットのパケットでは、イーサネットヘッダ部とデータ部に分けられる。イーサネットデータ部には上位層プロトコルである IP のパケットが格納されており、この IP パケットもヘッダ部とデータ部に分けられる。同じように、IP パケットのデータ部には、より上位層プロトコル、たとえば UDP のパケットが格納されている。このようなパケットの構造を、Wireshark の機能を用いて確認する。

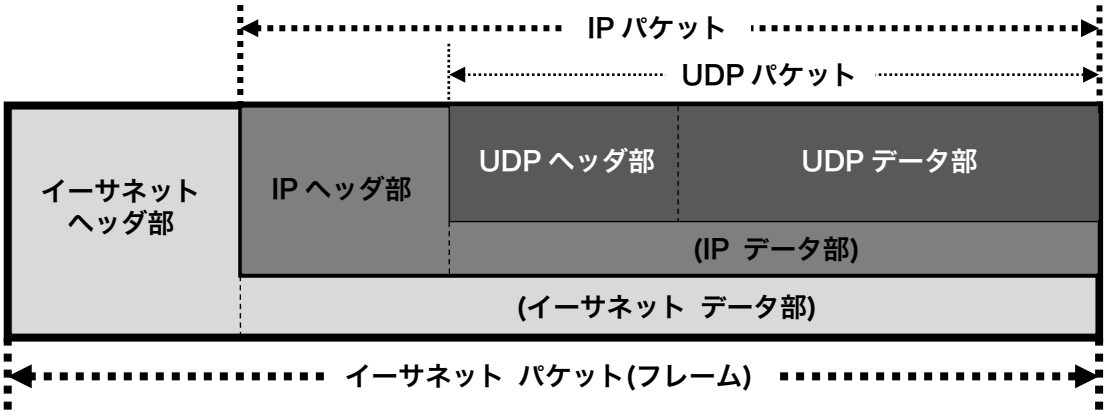


図 7　パケットの構造

パケットデータ部には、パケットの内容（実データ）が 16 進数ダンプ形式および ASCII 文字形式で表示されている。このデータの一部をクリックすると近辺が反転し、それらのデータに対応する項目の名称が、パケット詳細部内で反転する。

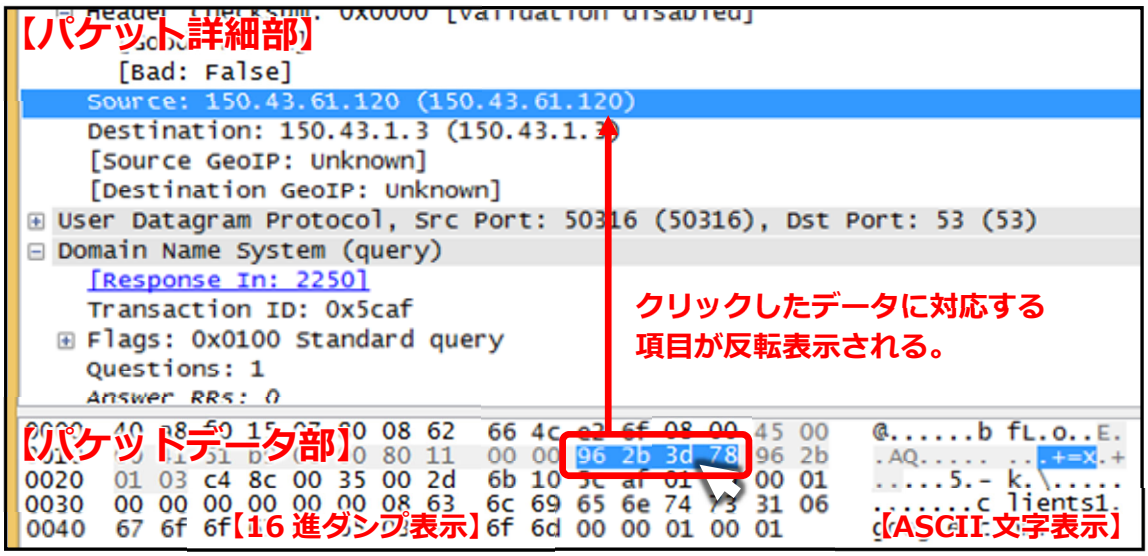


図 8　パケットデータ部の一部をクリックしたときの例

また、逆にパケット詳細部の項目名称をクリックし、反転させると、パケットデータ部の該当するデータが反転する。

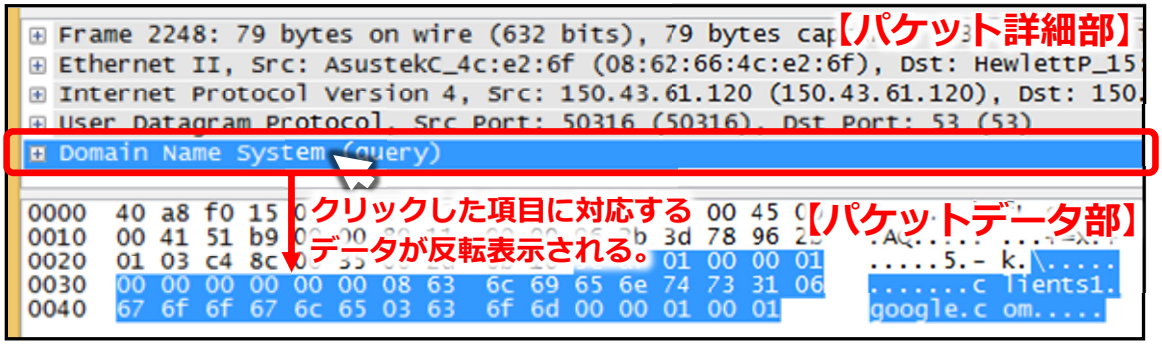


図 9　パケット詳細部の項目名称をクリックしたときの例

◆実験 3　自ホストから DNS サーバへ送信した、DNS 問い合わせ(**query**)パケットの構造を各プロトコル毎にわけ（イーサネット・IP・UDP・DNS）、結果を図で示す。

【手順】　パケット詳細部の各項目とパケットデータ部の実データの対応を調べ、実データ（16 進数のデータ）が、どのプロトコルに相当するデータなのかがわかるような図を作成する。図 7 に示したパケットの構造や、図 10 に示すパケット構造図の例も参考にする。
▼図を作成し、これを【レポート 5-2】とする。

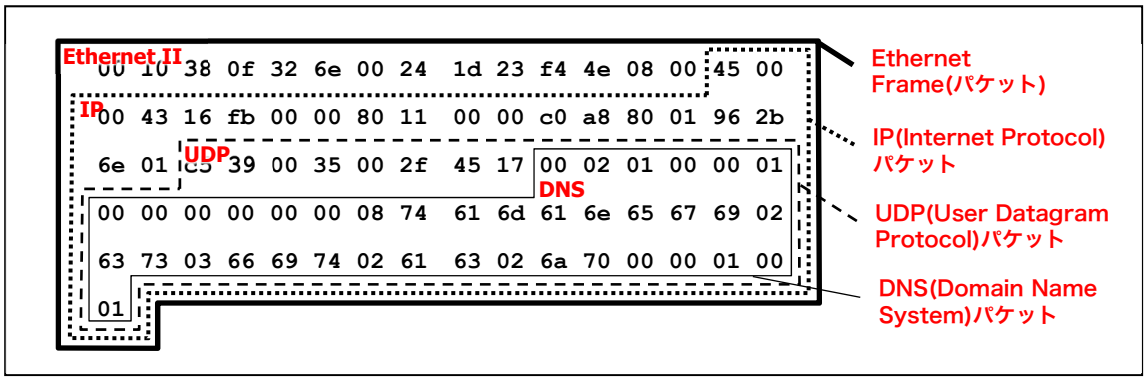


図 10　実データを用いたパケット構造図の例

※注　**この実験では、レスポンス(query response)パケットではなく、問い合わせ(query A)パケットを用いることに注意する。**

本実験で使用した Wireshark は、非常に多機能で強力なツールです。このようなツールは、便利な半面、使い方によっては不正な行為ができてしまいます。ネットワークの学習やトラブル解析などの正しい目的でのみ利用するようにしてください。

6. 不正アプリケーション（もどき）の調査（オプション）

近年、何らかの方法によりパソコン上に侵入した不正アプリケーション（マルウェア）が、情報をネットワークを介して外部に漏洩させる様な事例が増加している。本実験では、このような不正ソフトウェアを模したアプリケーションを実行し、そのアプリケーションの振る舞い（漏洩先や内容）について Wireshark を使用した調査を行い、応用力を身につける。

◆実験　調査対象のアプリケーション※を実行し、そのアプリケーションが送信したと考えられるパケットを Wireshark 上で見つける。そのパケットを詳しく調査し、アプリケーションの振る舞い（送信するタイミング／送信先 IP アドレス／使用プロトコル／送信先ポート番号／パケットに含まれるデータ 等...）を推測する。
その内容を、フリーフォーマットで記述する。【レポート 6 （オプション）】
※ **「デスクトップ > jikkenuser > 実験 III-調査対象アプリケーション > nazo.exe」を使用する。**

【パケットを絞り込むためのヒント】

- アプリケーションを含め、自パソコンから送信するパケットは全て、送信元 IP アドレスが自ホストの IP アドレスとなる。
- アプリケーション実行中にキャプチャする時間は、3〜5 分くらいで十分
- アプリケーション終了は Ctrl+C
- アプリケーションから送信するのは学内宛て（送信先 IP アドレスは 150.43.xx.xx）

※調査対象のアプリケーションが実際に送信するパケットは、万一外部に流出しても大きな影響がないようなデータやダミーの文字列等を使用しているので安心してください。

7. レポート

レポートは、A4 用紙を用い、次の指示にしたがって作成・提出する。

◆レポート形式

下図を参考にする。複数のメンバで同じ PC を使用して実験を行った場合は、レポート作成例の点線内のように、表紙に共同実験者を記入する（実験時、特に色々教えてもらったり助けてもらったりしたときは、その人を実験協力者として記入する）。共同実験者および実験協力者がいない場合は、点線内を記述する必要はない。また、PC 番号には、自分が実験時に着席した席の座席番号を用いる（掲示しているレイアウト図を参照する）。

レポートの本文は､本テキスト中【レポート n】と記載されている箇所の指示にしたがって作成する。

レポートは左上をステープラ（ホッチキス）等で綴じる。（両面印刷可／手書き可）

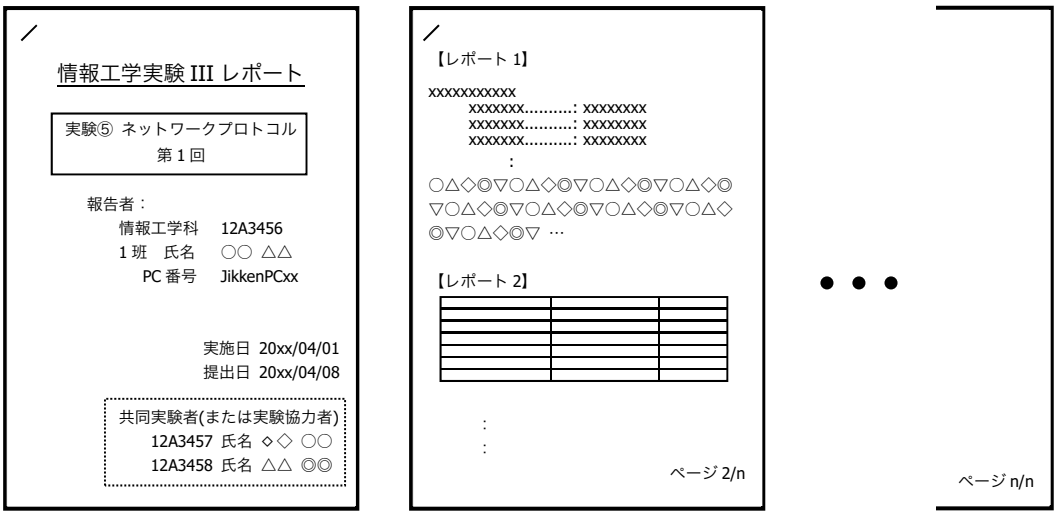


図 11　レポート作成例

◆提出締め切り・方法

次回の『情報工学実験 III』の実験日を提出締め切り日とする。実験室 4 内の『レポート提出 BOX』トレイへ提出する（実験室 4 施錠時には、C 棟 8F 相良研究室ドアポストへ）。