実験② ネットワークプロトコル　第 1 回

Rel. 20120409A

情報工学実験 III@実験室 4

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。

第 1 回　Windows プラットフォーム上での実験

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「個人用」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、実験中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　自席パソコンのネットワーク関連情報を調べる。

【手順 1】コマンドプロンプトを起動する。（『  （スタート）』-『すべてのプログラム』-『アクセサリ』-『コマンドプロンプト』と選ぶ）

【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 ローカルエリア接続：」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:  cen.ipc.fit.ac.jp    …【DNS サーバのホスト名】
Address:  150.43.110.1          …【DNS サーバの IP アドレス】

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)】
```

問い合わせに利用した 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、表を完成させる。

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
	情報処理センターサーバ	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)		

【手順】 コマンドプロンプトに『nslookup（調べたいホスト名 or IP アドレス）』と入力
▼ 結果を記録し、完成した表の全体を【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 xxx を問い合わせた結果、「＊＊＊（DNS サーバ）が xxx を見つけられません: zzz... 」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 アドレスが正しく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。

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プログラムである。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、問題の初期段階での切り分けを行うことができる。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、ルータ等がエラーを通知する】
        :
(デフォルトでは、ping パケットを 4 回送信した結果の表示後、統計情報を表示する。)
```

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、表を完成させる。

表 2　ping コマンドを使用した応答有無の調査

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
福工大 Web サイト	fitweb.ipc.fit.ac.jp	
情報処理センターサーバ	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	
不明なマシン	150.43.248.40	
(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 ）

【手順】　コマンドプロンプト画面に 『ping（ホスト名 or IP アドレス）』と入力
▼ 結果を記録し、完成した表の全体を【レポート 3】とする。

近年のウィルス・ワーム等の流行により、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、手動で行っていたが、DHCP(Dynamic Host Configuration Protocol)の普及により、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ことが一般的になっている。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 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
▼出力された内容のうち、「イーサネットアダプター ローカルエリア接続：」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 ローカルエリア接続：」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 ネットワークアナライザ プログラム -

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。

◆Wireshark プログラムの起動
（『スタート』-『すべてのプログラム』-『Wireshark』と選ぶ）
▼ プログラムが起動することを確認する。

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、つまり、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　Wireshark でキャプチャ中に、ブラウザ等で任意の Web サイトを閲覧し、その際に自動的に行われた、DNS 問い合わせ（ホスト名→IP アドレス変換）のパケットをみつける。（この、実験 1 の段階では、画面上で DNS パケットの行を見つけるだけで良い。見つけた後は、次の実験 2 へ進む。）

【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、IP が 150.43.で始まるアドレスになっているインタフェース（実験室内 PC の多くは「Realtek PCIe...」というインタフェース名になっている）の『Start』ボタンを押す（下図参照）。

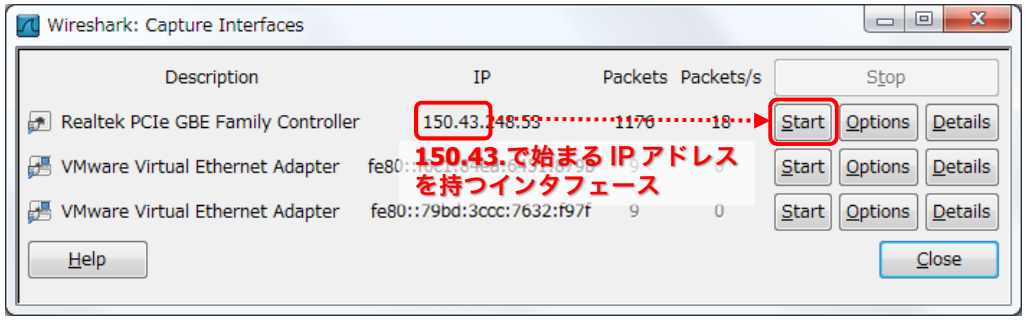

図 3　Wireshark: Capture Interfaces ダイアログ

▼ 同ダイアログが消え、Wireshark のメイン画面に戻り、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（画面上に、キャプチャしたパケットがリアルタイムに表示される）。

【手順 2】InternetExplorer（ブラウザ）を起動し、任意の Web サイトを閲覧する。

【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『  (Stop the running live capture)』ボタンを押す。

Wireshark のメイン画面の例を次に図示する。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ぶ。

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（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。

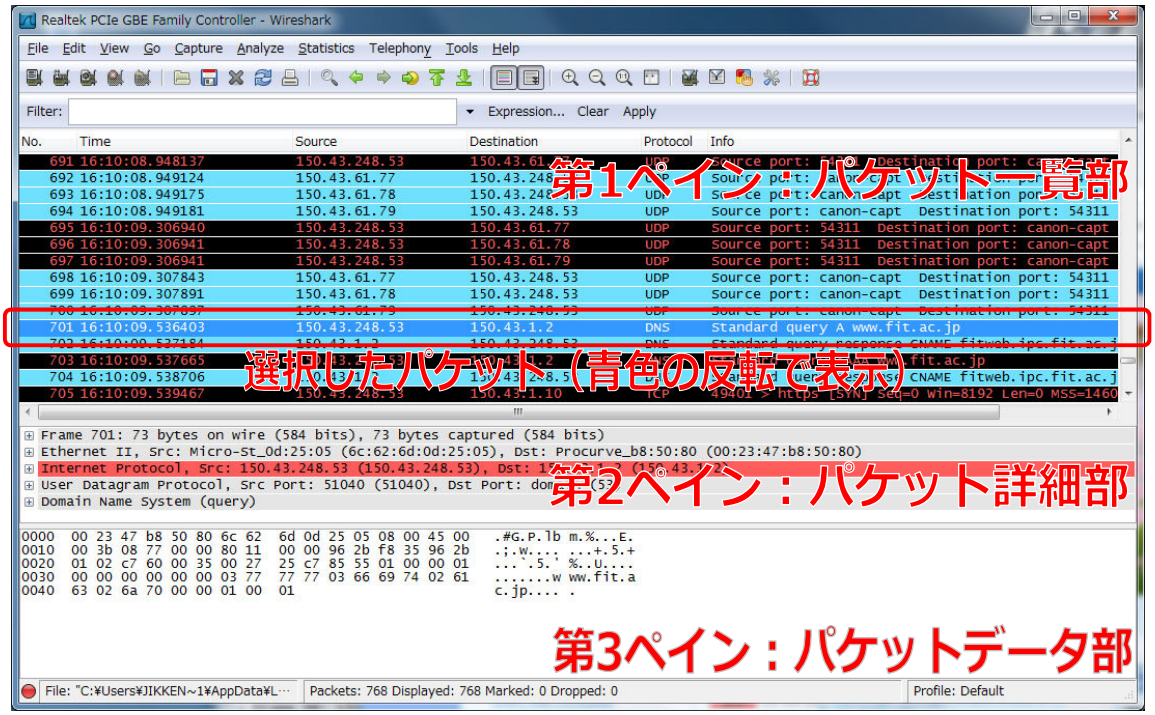

図 4　Wireshark のメイン画面の例（キャプチャ後）

▼次に、『Protocol』フィールドが『DNS』となっている行（パケット）を見つける。

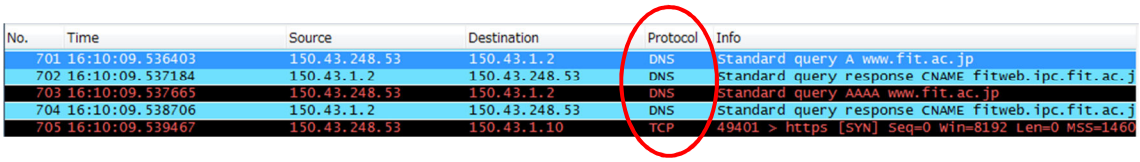

図 5　DNS パケットの例（この場合 4 つの DNS パケットが続いている）

ここで、『Info』フィールドが『Standard **query** 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』項目が『Standard query **response**…』で始まる DNS パケットが、DNS サーバから受信した、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。

※注　**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。**

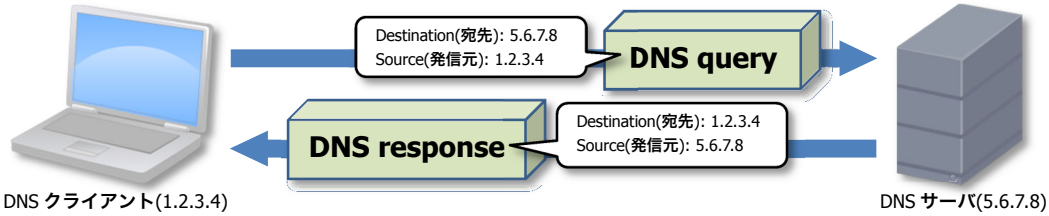

図 6　DNS クライアントとサーバ間でやりとりされるパケット

DNS サーバから受信した、レスポンス（query **response**）パケットの中には、回答のみでなく、元となった問い合わせの内容（ホスト名）とその回答（本名や IP アドレス）が含まれている（図 7 参照）。

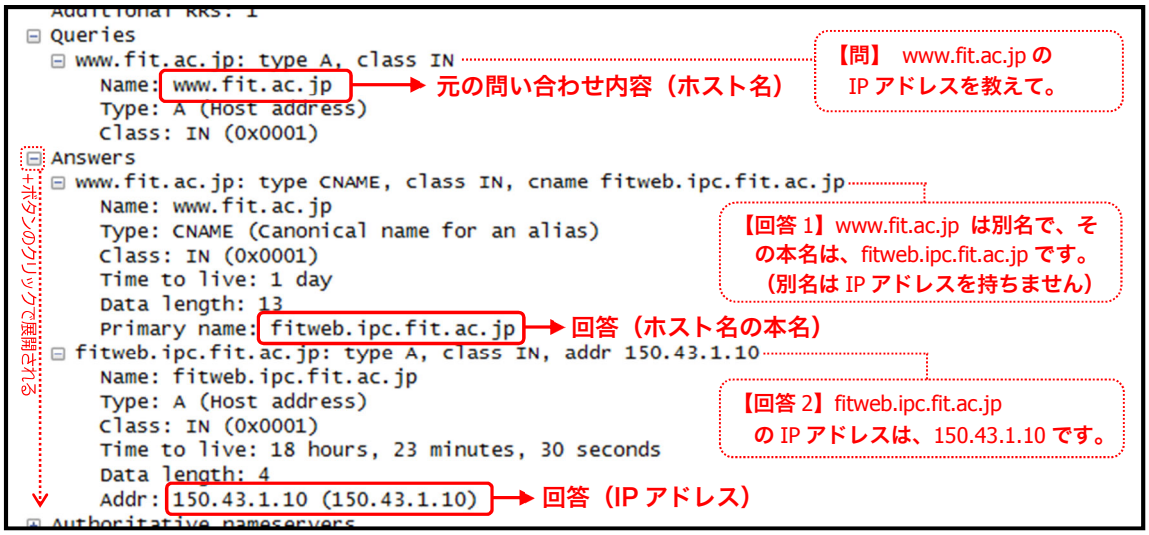

図 7　query response パケットの内容の例（パケット詳細部より）

◆実験 2　前実験でキャプチャしたデータを用いて、その中に含まれる、DNS サーバから受信したレスポンス（query **response**）パケットの内容を調べ、次表を完成させる。

表 3　DNS query response パケットの内容

元の問い合わせ内容（ホスト名）	
回答（ホスト名の本名）	
回答（IP アドレス）	

【手順】　DNS の query response パケットを選択し、そのパケット詳細部の『Domain Name System (response)』ツリーを開いて行き（左端の ⊞ ボタンのクリックで、より詳細な項目が展開される）、ホスト名や IP アドレスを見つける。

▼ 結果を記録し、完成した表の全体を【レポート 5-1】とする。

※注 1　回答内に複数の本名／IP アドレスが含まれる場合、最初に現れた本名／IP アドレスを表に記入する（すべて記入しても良い）。

※注 2　元の問い合わせ内容のホスト名自体が、本名に等しい（別名を持たない）場合も

ある。この場合、表の「回答（ホスト名の本名）」欄には「ー」（ハイフン）を記入する。

【参考】Web システムでは、www.xxx.jp といった代表的なホスト名は、別名（エイリアス）とし、その実体のサーバは内部的な本名を持っていることも多い（実体のサーバ開発・切り替えが容易になる）。また、大規模なシステムになると、別名 www.xxx.jp に対して、異なる本名を持つ実体サーバを複数台用意し、それらのサーバ群のうち 1 台が、順番に www.xxx.jp へのアクセスを担うことで、アクセス負荷を分散させたりしている（DNS のラウンドロビン機能）。

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出きる。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。

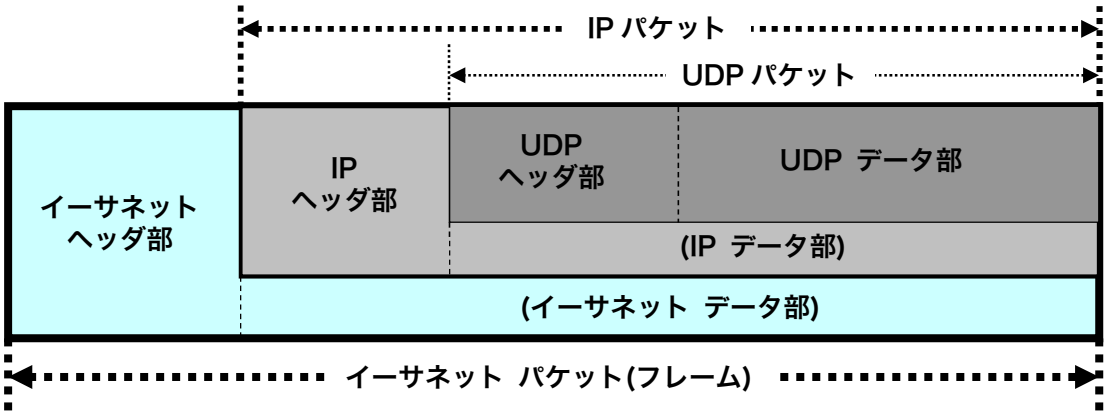

図 8　パケットの構造

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。

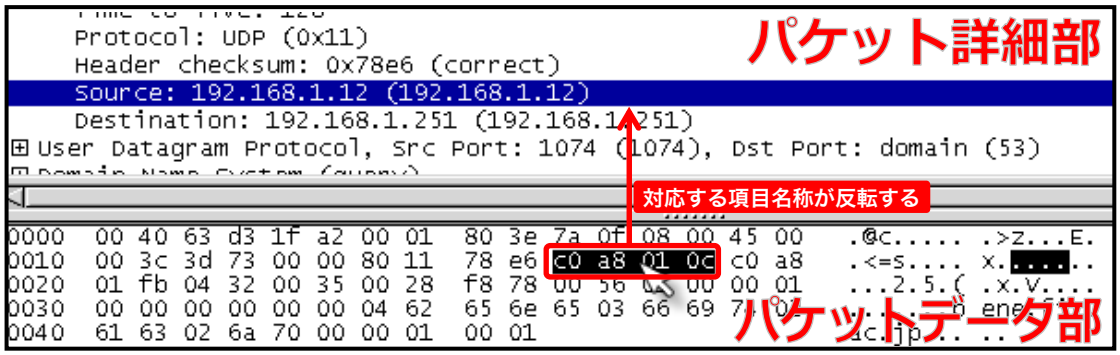

図 9　パケットデータ部の一部をクリックしたときの例

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。

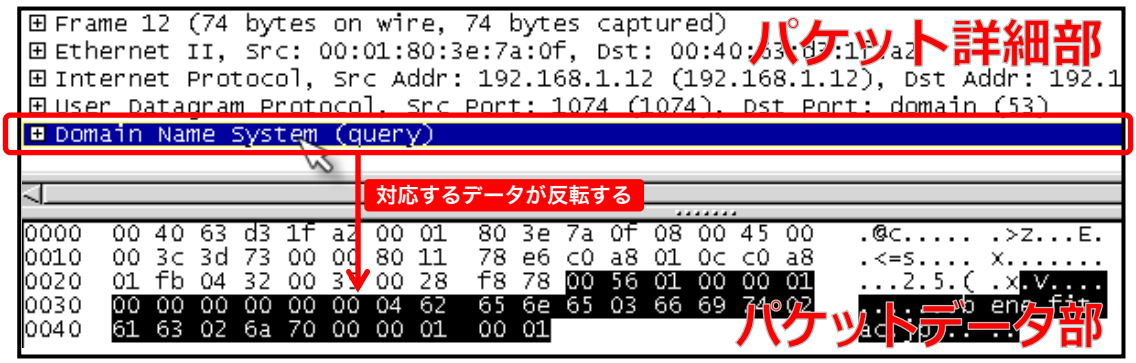

図 10　パケット詳細部の項目名称をクリックしたときの例

◆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 8 に示したパケットの構造や、図 11 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。

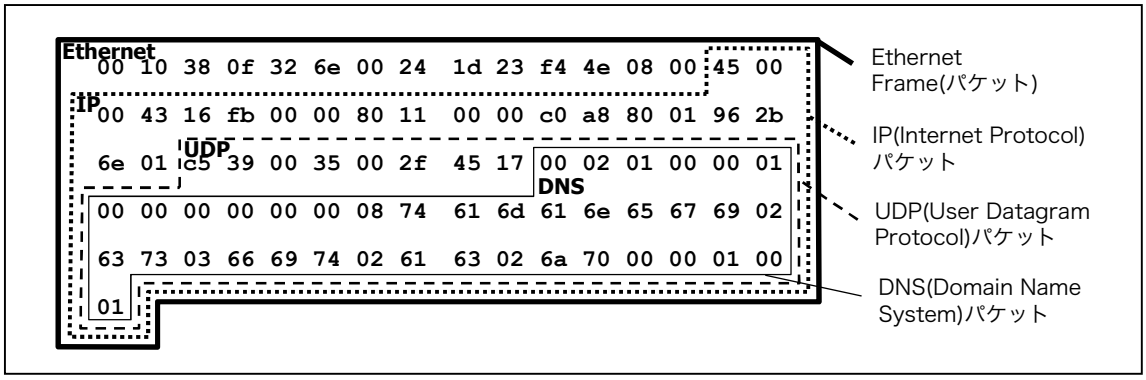

図 11　実データを用いたパケット構造図の例

※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. トラブルシューティング（オプション）

知り合いから、電話で「あるホームページ（サイト）が見れなくなったけど、どうすればいいと？」と助けを求められてしまったとする。

当然、たったそれだけの情報でトラブルが解決できるはずはない。このようなとき、

a) どのような追加質問・指示等（調査）を行えばよいか。

また、それによって得られた追加情報により、

b) 原因として考えられるのはどのような状況か。

さらに、

c) 解決するにはどう指示・回答すればよいか。

を考える。

◆考察　前述のサイトを閲覧できないというトラブルに関して、自分の経験や、今回学んだコマンド・ツール類の利用などによる調査、原因と解決方法を考える。

▼ a)〜c) の内容を下表の例にならってまとめる【レポート 6 （オプション）】。

a) **追加質問・指示等**	b) **考えられる原因**	c) **解決するには**
【例 1】 問題のサイト以外は見られるのか?	(Yes) そのサイト側の障害の可能性がある。	サイト管理者に連絡するか、回復するまで待つ。
	(No) 使用している PC 側の障害の可能性がある。	さらなる調査が必要。
【例 2】 最近そのサイトにアクセスしたのはいつ?	数年前など、ずいぶん昔であれば、ホスト名等のアドレスが変更になった可能性がある。	google エンジンなどで改めて検索する。
【例 3】 nslookup [サイトのホスト名] を実行させる。	IP アドレスが返却されなければ、DNS の仕組みに問題が生じていると考えられる。	さらなる調査が必要。 （特に DNS 障害の原因）

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、座席番号には、自分が実験時に着席した席の座席番号を記入する（黒板の座席レイアウト図か、Windows の『コントロールパネル』-『システムとセキュリティ』-『システム』-『コンピューター名』を参照する）。

レポートの本文は、本テキスト中【レポート n】と記載されている個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）等で綴じて提出する。

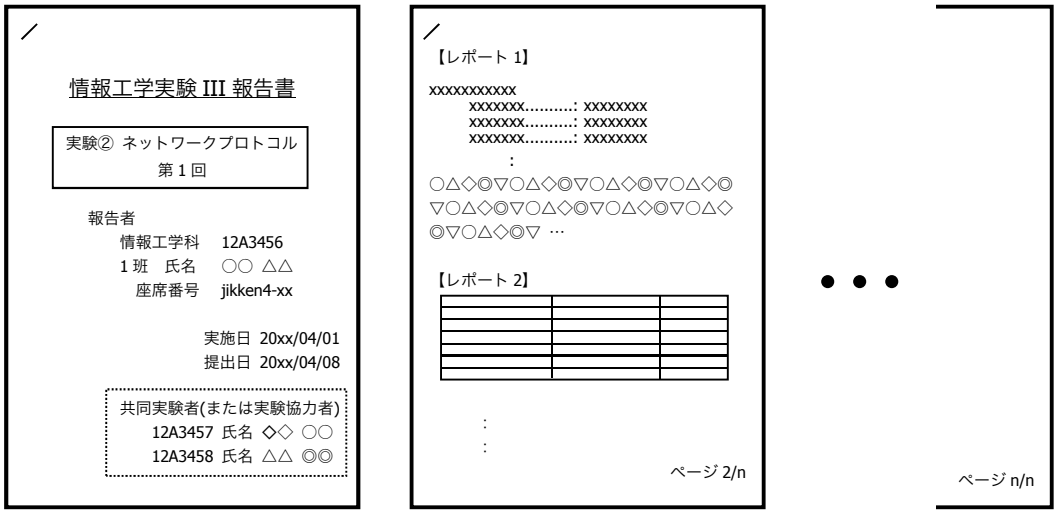

図 12　レポート作成例

◆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』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）。