実験② ネットワークプロトコル　第 1 回

Rel. 20080416A

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

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"IP Address"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、ホスト名と IP アドレス

と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:¥Documents and Settings¥USER> nslookup www.fit.ac.jp

Server:  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】   } DNS サーバに関する情報【今回は不要（参考用）】

Name:    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)】            } 問い合わせに対する回答情報
```

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。

【例】

コンピュータの種類	ホスト名（本名）	IP アドレス
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こと。

※注 2　DNS サーバへ問い合わせた結果、「＊＊＊ xxx can't find yyy：zzz... 」と返却されることがある。これは、DNS データベース上に問い合わせに対する回答が正し

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、問題の早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:¥Documents and Settings¥USER> ping xxx.ac.jp

Pinging xxx.ac.jp [nn.nn.nn.nn] with 32 bytes of data:

Reply from nn.nn.nn.nn: bytes=32 time=3ms TTL=250
       :                                          【応答がある場合】
       :
Request timed out.
       :                                          【応答がない場合】
       :
```

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。

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.□	
不明なマシン	150.43.248.40	
(任意のサイト 1)		
(任意のサイト 2)		

【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・ルータ類によって通さない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、経路上でブロック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 -

すこし昔までは、コンピュータの IP アドレス等の設定は、手動で行われていたが、DHCP(Dynamic Host Configuration Protocol)の普及により、ネットワーク関連の設定が自動で取得できるようになり、プラグ&プレイが実現された。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、IP アドレス等の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い、IP アドレスを割り当ててもらう。

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
▼ IP アドレス欄に 0.0.0.0 と表示されることを確認する。

【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
▼ しばらくたった後､IP 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
▼ “Lease Obtained”の日時を記録し、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 - Ethereal ネットワークアナライザ プログラム -

ここでは、Ethereal 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。

◆Ethereal プログラムの起動

（『スタート』-『すべてのプログラム』-『Ethereal』-『 Ethereal』と選ぶ）

▼ Ethereal が起動することを確認する。

Ethereal 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ボタンを押すまでの間、パソコンの NIC（ネットワークインタフェースカード）上を通過するパケットをキャプチャし続ける。

◆実験 1　Ethereal 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、その際に内部で自動的に行われた、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次の実験 2 へ進んでよい。）

【手順 1】キャプチャを開始する。

Ethereal ツールバー左端の『 』ボタンを押し、出現した『Ethereal: Capture Options』ダイアログで『OK』ボタンを押す。

▼ 『Ethereal: Capture』ダイアログ（下部に『Stop』ボタンがある）が出現し、キャプチャが開始されたことを確認する。

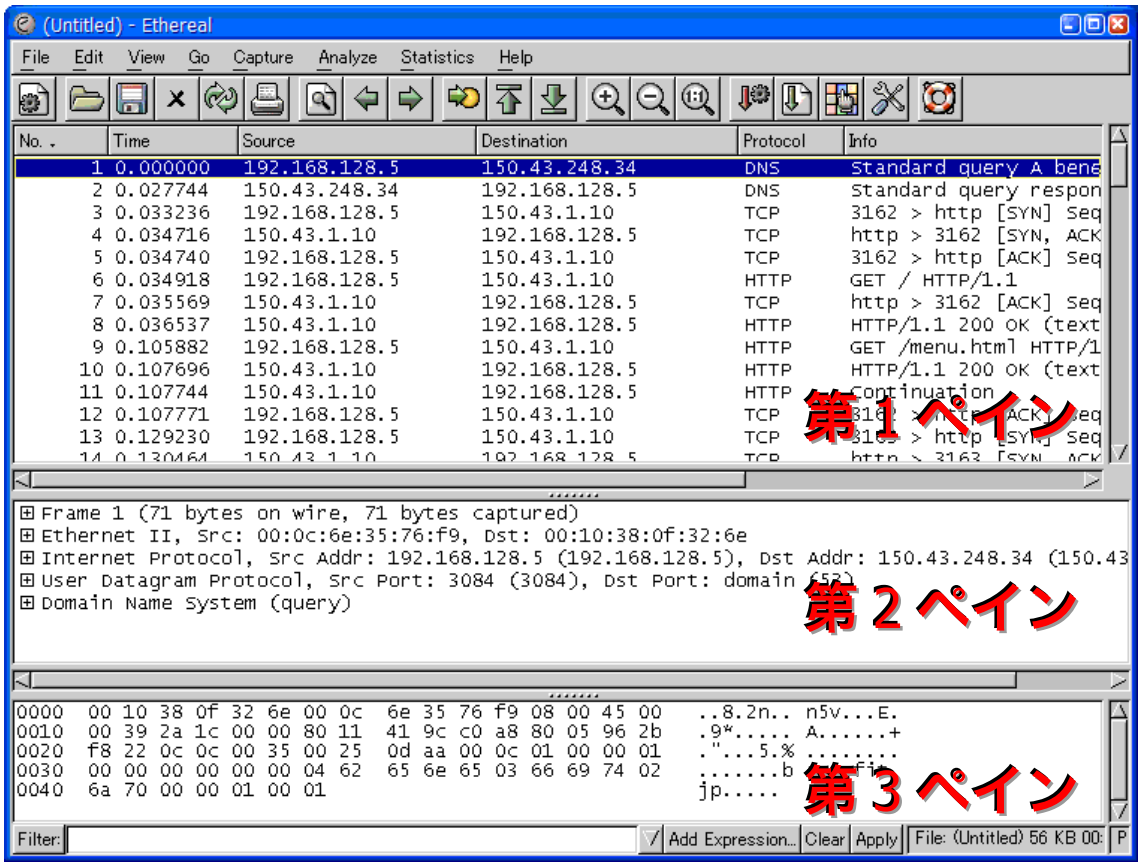
【手順 2】InternetExplorer を起動し、任意の Web サイトを閲覧する。

【手順 3】キャプチャを終了する。

『Ethereal: Capture』ダイアログの『Stop』ボタンを押す。

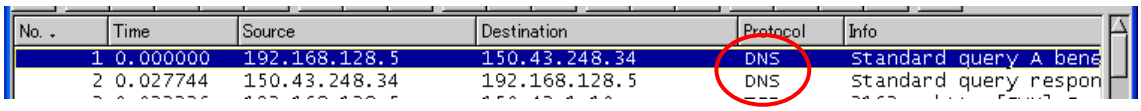
▼ 次のような Ethereal のメイン画面が表示されることを確認する。

ここで、ネットワーク上で送受信されている 1 つのパケットは Ethereal の第 1 ペイン内の 1 行に相当する。また、第 1 ペイン内で選択したパケット（反転させた行）の詳細が第 2 ペインに表示される。



Ethereal キャプチャ終了後のメイン画面

▼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。

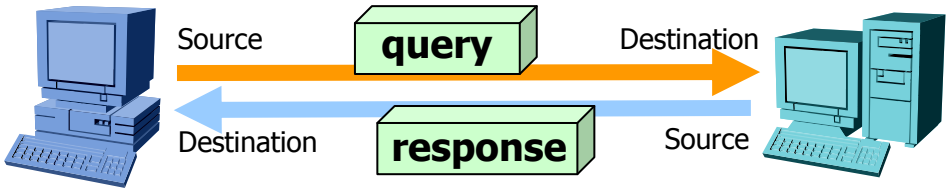


第 1 ペイン画面例

ここで、『Info』フィールドが『Standard **query** A…』で始まる 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。

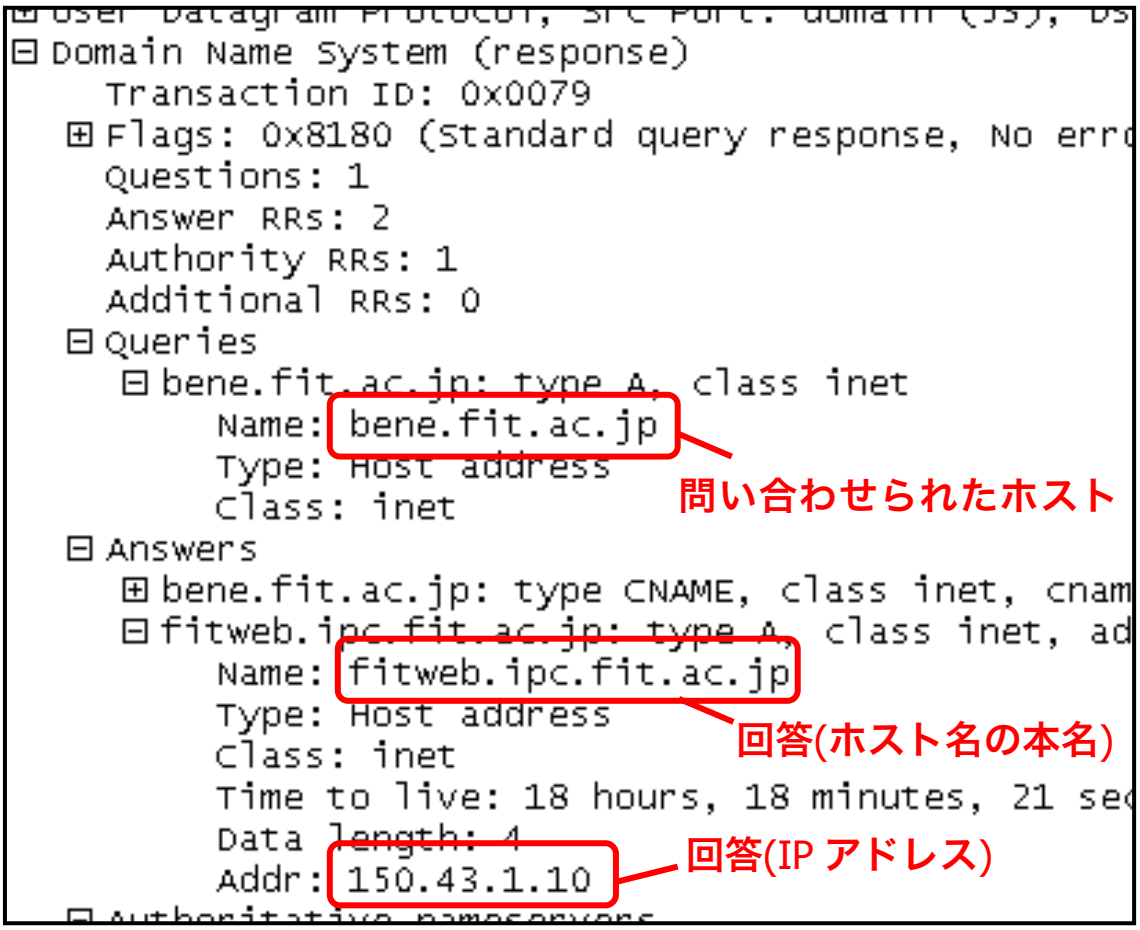
また、『Info』項目が『Standard query **response**…』で始まる DNS パケットが、 DNS サーバから受信した、レスポンス（query response）であり、『Source』と『Destination』のアドレスが、前述の問い合わせ（query）の逆になっていることがわかる。

※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。



DNS クライアント（左側）と DNS サーバ（右側）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、問い合わせられた内容（ホスト名）と、その回答（本名や IP アドレス）が含まれている（下図）。



query response パケットの内容

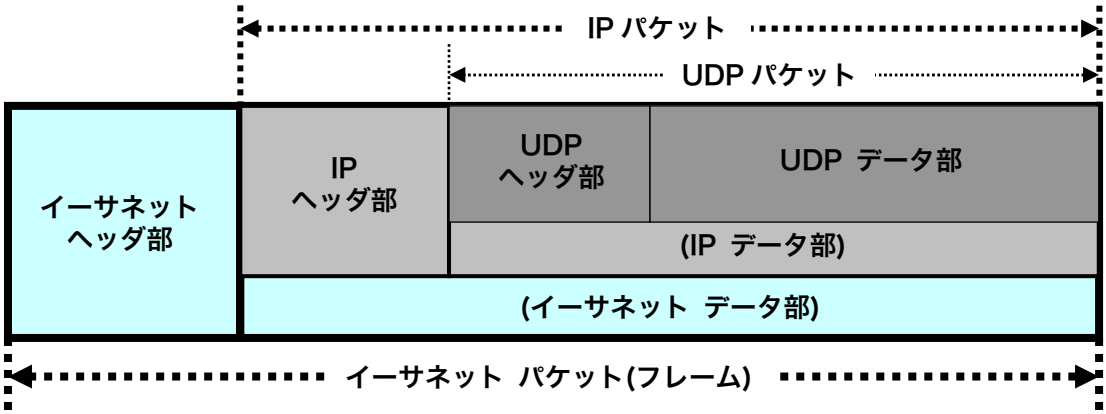
◆実験 2　前実験でキャプチャしたデータを用いて、その中に含まれる、DNS サーバから受信したレスポンス（query **response**）パケットの内容を調べ、次表を完成させる。

問い合わせられた内容（ホスト名）	
問い合わせの回答（ホスト名の本名）	
問い合わせの回答（IP アドレス）	

【手順】 Ethereal 画面の第 2 ペイン中の『Domain Name System (response)』ツリーを開き、必要な項目を探す。

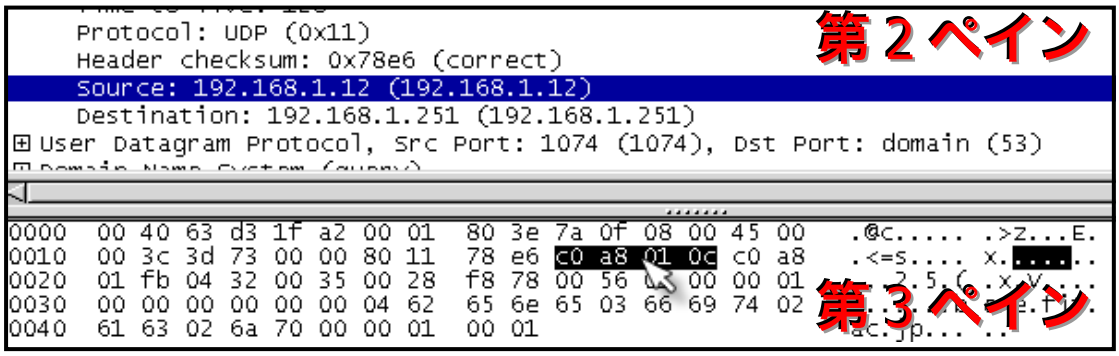
▼ 結果を記録し、完成した表の全体を【レポート 5-1】とする。

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。このデータ部は上位層プロトコルの IP パケットとなっており、IP パケットもさらに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は、より上位層プロトコル、たとえば UDP のパケットとなっている。このようなパケットの構造を、Ethereal の機能を用いて解析する。



パケットの構造

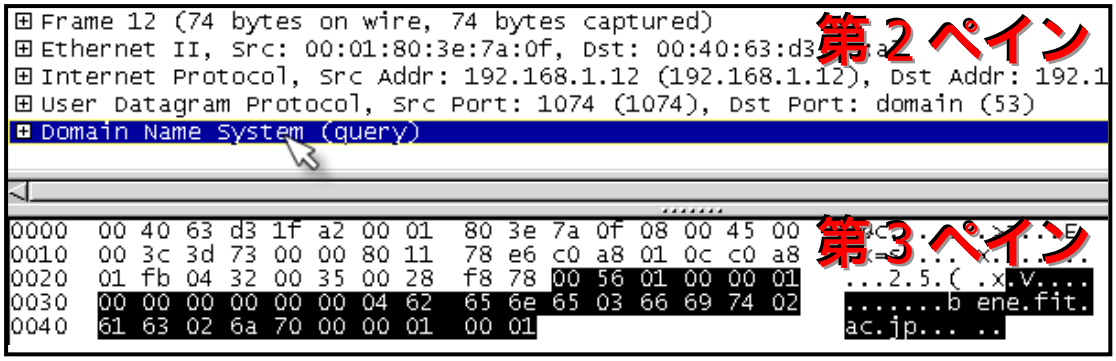
Ethereal 画面の第 3 ペインには、パケットの内容（生データ）が 16 進数ダンプ形式で表示されている。このデータの一部をクリックすると近辺のフィールドが反転し、そのフィールドに対応する項目の名称が、第 2 ペイン中に反転する。



第 3 ペインのフィールドをクリックしたときの例

また、逆に第 2 ペイン中の項目名称をクリックし、反転させると、第 3 ペインの該当するフィールドが反転する。（なお、Ethereal の第 2 ペインに表示される項目名称は、各プロトコルのヘッダ部の名称であり、各プロトコルのデータ部は特に明示されず、上位層プロト

コルのヘッダ部が表示される。）



第 2 ペインの項目名称をクリックしたときの例

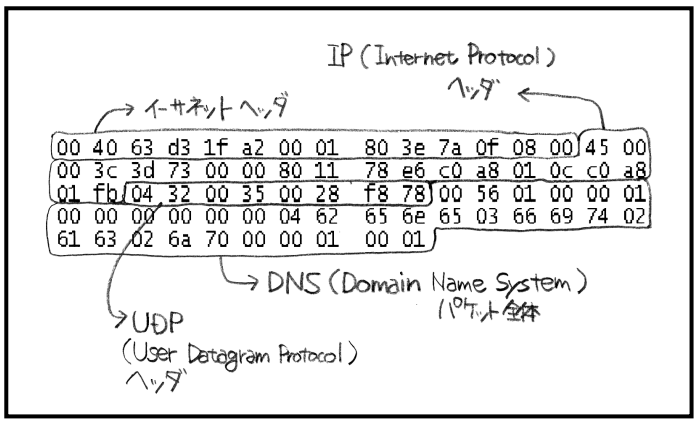
次の実験では、上記機能を利用して、パケットの構造の解析を行う。

◆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**)パケットの構造を解析し、結果を図で示す。

【手順】　Ethereal 第 2 ペイン中の各項目と第 3 ペイン中の生データの対応を調べ、生データ（16 進数のデータ）が、どのプロトコルに相当するのかがわかるような図を考える。

▼ 図を完成させる【レポート 5-2】。

◎ わかりやすい図になるように工夫することが、このレポートのポイントとなる。



簡単な図の例（あまりわかりやすくない例）

※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)パケットを用いることに注意する。

★★★　Ethereal 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。

　なお、現在フリーソフトとしての Ethereal の開発は終了しており、その実質的な後継ソフトは、**WireShark** という名称になっています(商標登録の関係上、Ethereal という名称をフリー版が継続使用するのが難しくなったため)。

6. 考察：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？」とヘルプ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）

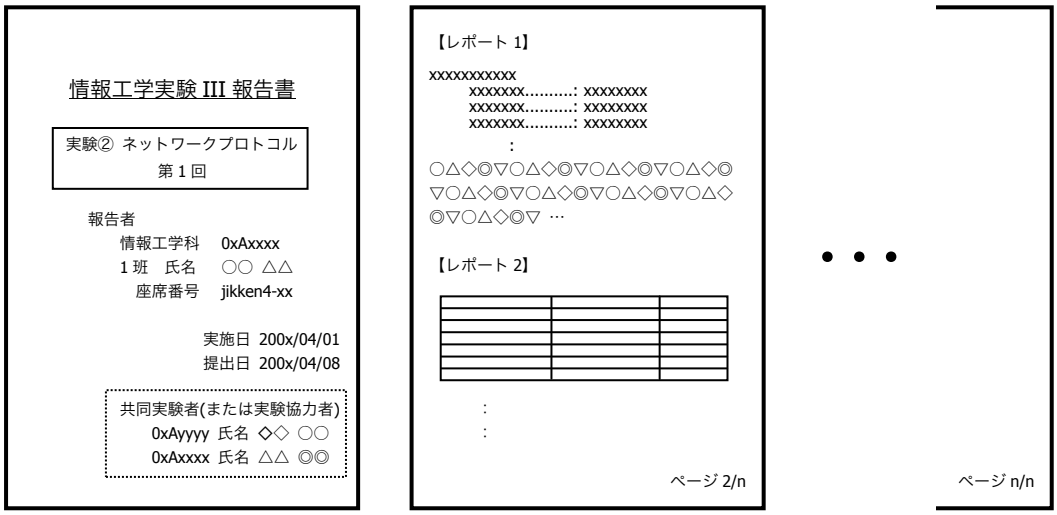
7. レポート

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）。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 起動中であれば『コントロールパネル』-『システム』-『コンピュータ名』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。



レポート作成例

◆提出締め切り・方法

次週の『情報工学実験 III』の実験開始前に、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）。