CHAPTER 2
APPLICATION LAYER

Chapter Summary

The Application Layer (also called layer 5) is the software that enables the user to perform useful work. The software at the application layer is the reason for having the network because it is this software that provides the business value. This chapter examines the five fundamental types of application architectures used at the application layer (host-based, client-based, client-server, cloud-based, peer to peer). It then looks at the Internet and the primary software application packages it enables: the Web, email, Telnet, and instant messaging.

Learning Objectives

After reading this chapter, students should be able to:

- understand host-based, client-based, client-server, cloud-based, and peer-to-peer application architectures
- understand how the Web works
- understand how email works
- be aware of how Telnet and instant messaging works

Key Terms

application architecture
application logic
client-based architecture
client-server architecture
cloud computing
cluster
data access logic
data storage
desktop videoconferencing
distributed computing model
dumb terminal
email
green computing
H.320
H.323
host-based architecture
HTTP request
HTTP response
Hypertext Markup Language (HTML)
Hypertext Transfer Protocol (HTTP)
instant messaging (IM)
Internet
Internet Message Access Protocol (IMAP)
mail transfer agent
mail user agent
mainframe
middleware
MPEG-2
Multipurpose Internet Mail Extension (MIME)
network computer
n-tier architecture
peer-to-peer architecture
personal computer
Post Office Protocol (POP)
presentation logic
protocol
request body
request header
request line
response body
response header
response status
scalability
server virtualization
Simple Mail Transfer Protocol (SMTP)
SMTP header
SMTP body
Telnet
terminal
thick client
thin client
three-tier architecture
transaction terminal
two-tier architecture
uniform resource locator (URL)
videoconferencing
virtual server
World Wide Web
Web browser
Webcasting
Web server

Chapter Outline

1. INTRODUCTION
2. APPLICATION ARCHITECTURES
    a. Host-Based Architectures
    b. Client-Based Architectures
    c. Client-Server Architectures
    d. Cloud Computing Architectures
    e. Peer-to-Peer Architectures
    f. Choosing Architectures
3. WORLD WIDE WEB
    a. How the Web Works
    b. Inside an HTTP Request
    c. Inside an HTTP Response
4. ELECTRONIC MAIL
    a. How E-Mail Works
    b. Inside an SMTP Packet
    c. Attachments in Multipurpose Internet Mail Extension
5. OTHER APPLICATIONS
    a. Telnet
    b. Instant Messaging
    c. Videoconferencing
6. IMPLICATIONS FOR MANAGEMENT
   SUMMARY

Answers to Textbook Exercises

1. What are the different types of application architectures?

   Host-based (all processing done on host system and all data on host with terminals providing access), client-based (with processing done on client and all data stored on server), and client-server (balanced processing; usually host provides data access and storage while the client provides application and presentation logic).

2. Describe the four basic functions of an application software package.

   Data storage, data access logic, application logic, and presentation logic.

3. What are the advantages and disadvantages of host-based networks versus client-server networks?

	Host-based	Client-server
Advantages	Centralized security Integrated architecture from single vendor Simpler, centralized installation	Balanced processing demands Lower cost; inexpensive infrastructure Can use software and hardware from different vendors Scalability
Disadvantages	Having all processing on host may lead to overload Cost of software and upgrades; expensive infrastructure Terminal totally dependent on server	Problems with using software and/or hardware from different vendors More complex installation or updating (although automated installation software helps greatly in this area).

4. What is middleware and what does it do?

   Middleware manages client-server message transfer and shields application software from impacts of hardware changes. Middleware provides standard communication between products of different vendors through translation.

5. Suppose your organization was contemplating switching from a host-based architecture to client-server. What problems would you foresee?

   Infrastructure supporting cabling hardware and software will need to be redesigned to support the client-server approach to the architecture. Someone would need to be designated to manage what would now become the local area network, so there may be a personnel impact. Security would be one area of concern, since processing can be done on individual workstations. There may be somewhat greater complexity of upgrades, although newer software is reducing the impact of this kind of problem.

6. Which is less expensive: host-based networks or client-server networks? Explain.

   Client-server networks are less expensive because in a competitive market involving multiple vendors, software and hardware upgrades cost substantially less. Upgrades for host-based networks are generally very expensive, and occur in what is generally termed a "step function," meaning requiring large, discrete steps in expenditure. LANs have the ability to be deployed with a smoother cost curve in less severe increments.

7. Compare and contrast two-tiered, three-tiered, and *n*-tiered client server architectures. What are the technical differences, and what advantages and disadvantages do each offer?

   Two-tiered architectures have only clients and servers.
   Three-tiered architectures typical separate (1) presentation logic, (2) application logic, and (3) and data access logic and storage.
   In n-tiered architecture more than one tier may be used to support application logic, typically due to a Web server tier being included.
   Three-tiered or n-tiered architectures place a greater load on the network, but balances server load better and is more scalable.

8. How does a thin client differ from a thick client?

   Thick clients support all or most application logic while thin clients support little or no application logic. Development and maintenance costs for more complex thick-client environments can be higher than for thin clients.

9. What are the benefits of cloud computing?

   Benefits include gaining access to experts to manage the cloud, potentially lower costs, scalability, and pay-as-you-g0.

10. Compare and contrast the three cloud computing models.

    See Figure 2-7

11. What is a network computer?

    A network computer supports Internet access but has no hard disk local storage.

12. For what is HTTP used? What are its major parts?

    The standard protocol for communication between a Web browser and a Web server is Hypertext Transfer Protocol (HTTP). An HTTP request from a Web browser to a Web server has three parts. Only the first part is required; the other two are optional.
    - the request line, which starts with a command (e.g., GET), provides the URL, and ends with the HTTP version number that the browser understands.

- the request header, which contains a variety of optional information such as the Web browser being used (e.g., Internet Explorer), the date, and a userid and password for use if the Web page is password-protected.
- the request body, which contains information sent to the server, such as information from a form.

The format of an HTTP response from the server to the browser is very similar to the browser request. It has three parts, but only the last part is required; the first two are optional:

- the response status, which contains the HTTP version number the server has used, a status code (e.g., 200 means OK, 404 means page not found), and reason phrase (a text description of the status code)
- the response header, which contains a variety of optional information such as the Web server being used (e.g., Apache), the date, the exact URL of the page in the response body, and the format used for the body (e.g., HTML)
- the response body, which is the Web page itself.

13. For what is HTML used?

HTML is the language in which web pages are created. The response body of an HTTP response can be in any format, such as text, Microsoft Word, Adobe PDF, or a host of other formats, but the most commonly used format is HTML. The major parts of HTML are the heading (denoted by the <head> tag) and the body (denoted by the <body> tag) of the response.

14. Describe how a Web browser and Web server work together to send a Web page to a user.

In order to get a page from the Web, the user must type the Internet Uniform Resource Locator (URL) for the page he or she wants, or click on a link that provides the URL. The URL specifies the Internet address of the Web server and the directory and name of the specific page wanted. In order for the requests from the Web browser to be understood by the Web server, they must use the same standard protocol. The standard protocol for communication between a Web browser and a Web server is Hypertext Transfer Protocol (HTTP).

15. Can a mail sender use a two-tier architecture to send mail to a receiver using a three-tier architecture? Explain.

Yes. With e-mail, users with the two-tier architecture will use the user agent software to interface with their email server, which will send out web based, SMTP packets to the far end receiver's server computer with mail server software. The server at the far end will issue an IMAP or SMTP packet to the receiver's server computer, which will then arrive at the receiver when they ask for the email with an HTTP request to the web based email application. Thus, a 2-tiered system easily interfaces with a three-tiered architecture over the internet using the appropriate protocols.

16. Describe how mail user agents and message transfer agents work together to transfer mail messages.

    The sender of an e-mail uses a user agent (an application layer software package) to write the e-mail message. The user agent sends the message to a mail server that runs a special application layer software package called a message transfer agent. These agents read the envelope and then send the message through the network (possibly through dozens of mail transfer agents) until the message arrives at the receiver's mail server. The mail transfer agent on this server then stores the message in the receiver's mailbox on the server. When the receiver next accesses his or her e-mail, the user agent on his or her client computer contacts the mail transfer agent on the mail server and asks for the contents of the user's mailbox. The mail transfer agent sends the e-mail message to the client computer, which the user reads with the user agent.

17. What roles do SMTP, POP, and IMAP play in sending and receiving e-mail on the Internet?

    SMTP defines how message transfer agents operate and how they format messages sent to other message transfer agents. The SMTP standard covers message transmission between message transfer agents (i.e., mail server to mail server). A different standard called Post Office Protocol (POP) defines how user agents operate and how messages to and from mail transfer agents are formatted. POP is gradually being replaced by a newer standard called Internet Mail Access Protocol (IMAP). While there are several important technical differences between POP and IMAP, the most noticeable difference is that before a user can read a mail message with a POP user agent, the e-mail message must be copied to the client computer's hard disk and deleted from the mail server. With IMAP, e-mail messages can remain stored on the mail server after they are read.

18. What are the major parts of an e-mail message?

    The major parts of an e-mail message are:
    - the header, which lists source and destination e-mail addresses (possibly in text form (e.g., "Susan Smith") as well as the address itself (e.g., smiths@robert-morris.edu)), date, subject, and so on
    - the body, which is the message itself.

19. What is a virtual server?

    A virtual server is one computer that acts as several servers. Using special software like Microsoft Virtual PC, WMWare, or VirtualBox, several operating systems are installed on the same physical computer so that one computer appears as several different ones on the network.

20. What is Telnet, and why is it useful?

    Telnet enables users on one computer to login into other computers on the Internet. Once Telnet makes the connection from the client to the server, a user can login into the server or host computer in the same way as that person would if they dialed in with a modem; the user must

know the account name and password of an authorized user. Telnet enables a person to connect to a remote computer without incurring long distance telephone charges.

Telnet can be useful because it enables access to servers or host computers without sitting at the dedicated computer's keyboard. Most network managers use Telnet to work on their organization's servers, rather than physically sitting in front of them and using the keyboards.

21. What is cloud computing?

    With cloud computing, a company contracts with another firm to provide software services over the Internet, rather than installing the software on its own servers. The company no longer buys and manages its own servers and software, but instead pays a monthly subscription fee or a fee based on how much they use the application.

22. Explain how instant messaging works.

    An instant messaging (client) communicates with an IM server application. Once a user is online, the server application can monitor connections so that multiple pre-identified clients can be notified and decide to participate in real-time messaging. IM may include video or audio. Video exchange, of course, requires cameras. Underlying this application requires a full-duplex connection between destination and host.

23. Compare and contrast the application architecture for videoconferencing with the architecture for e-mail.

    Videoconferencing must deliver real-time services demanding high capacity data transfer for both image and voice transmission. Specialized hardware (and even rooms) may be required. E-mail messages (typically without large attachments) are relatively small by comparison, can be received by any Internet-capable computer, and do not have to be consumed in real time.

24. Which of the common application architectures for e-mail (two-tier client-server, Web-based) is "best"? Explain.

    The best architecture for email can depend on how one wants to use e-mail. If a person wants to be able to access their e-mail from anywhere, then Web-based is best. If the person wants professional backup and storage within an organization, then two-tier client-server is best. If the person wants storage of e-mail strictly under their control and they also want to be able to access their e-mail files off-line when there is a network service interruption, then host-based is best. Employers may choose to use client-server architecture for email access within the organization and Web-based architecture for access to the same system for those times when employees are outside the company (at home, at another business, or on travel).

25. Some experts argue that thin-client client-server architectures are really host-based architectures in disguise and suffer from the same old problems. Do you agree? Explain.

    While thin client have substantially less application logic than thick client, they have sufficient application logic (as, for example, a Web browser possibly with Java applets) to participate in a client-server relationship. The older host-based terminals did not even have this much application logic. While thin-client use today reflects some level of return to a more centralized approach, the client is likely served by multiple servers (and even multiple tiers), rather than a single large host server as in the past. Thus, the two approaches are similar, but not exact, from a technological design perspective.

Mini-Cases

I. Deals-R-Us Brokers (Part 1)

Fred's information systems department has presented him with two alternatives for developing the new tools. The first alternative will have a special tool developed in C++ that clients will download onto their computers to run. The tool will communicate with the DRUB server to select data to analyze. The second alternative will have the C++ program running on the server; the client will use his or her browser to interact with the server.

a) Classify the two alternatives in terms of what type of application architecture they use.
b) Outline the pros and cons of the two alternatives and make a recommendation to Fred about which is better.

The alternatives are shown in the text as Figures 2-2 (client-based) and 2-3 (two-tier client-server).

Client-based is simple; however all data must travel to the client for processing, thus giving the potential for speed delays over the network.

Client-server provides processing on the server, which could be an advantage if the data to be processed also resides on the server; yet, because it involves heterogeneous software, this can be a significant disadvantage in terms of interoperability.

II. Deals-R-Us Brokers (Part 2)

Dears-R-Us Brokers has decided to install a new e-mail package. One vendor is offering an SMTP-based two-tier client server architecture. The second vendor is offering a Web-based e-mail architecture. Fred doesn't understand either one, but thinks the Web-based one should be better because, in his words "the Web is the future."

a) Briefly explain to Fred, in layman's terms, the differences between the two.
b) Outline the pros and cons of the two alternatives and make a recommendation to Fred about which is better.

a) If they host the email in-house using Microsoft Exchange Server, this means that they purchase a physical computer to use as a mail server and install Microsoft Server as the operating system. Then, they will need to install the Microsoft Exchange Server software

which will allow the server to be used as a mail server. The network administrator at DRUB can then configure and manage the email user accounts, etc himself. The second solution is to use one of the cloud-based providers and completely outsource the company email. Two examples are Gmail and GoDaddy. With each of these services, the DRUB will pay a monthly fee for one of the providers to configure and manage the mail servers for them.

b) *Each of these options has their advantages and disadvantages. A few of these include:*

In-house advantages: control, potentially lower cost
In-house disadvantages: more work to do, potentially less expertise available
Outsourcing advantage: potentially lower cost, better service, less work to do in-house
Outsourcing disadvantages: loss of control, potentially higher costs

III. Accurate Accounting

Accurate Accounting managing partner Diego Lopez asks: Why can't IM work as simply as e-mail? Will the new videoconferencing software and hardware work as simply as e-mail, or will it be IM all over again? Prepare a response to his questions.

E-mail standards enable it to be used easily between companies. Lack of IM standards means that several competing protocols exist. This problem will be overcome as commercial interests push for standardization or development of middleware that enables disparate systems to talk to one another. The same pattern of innovation will likely happen that is typical of all new technologies. At present, there are large corporate concerns over the security aspects of externally based IM software deployments within an organization's boundaries, limiting the use of IM packages in some organizations until these concerns are mitigated.

IV. Ling Galleries

How can the Internet help gallery owner Hoard Ling with his two new galleries?

There are a variety of ways the Internet could help Mr. Ling. He could develop a website where his paintings would be featured and some additional information about the artist would be displayed for potential buyers to learn and explore more about the works. Further, the website could include an e-commerce function whereby visitors would be able to order prints of paintings they like. The site could help Mr. Ling track customer tastes so that he can better understand the types of paintings that sell well, thus allowing the business to develop while matching future production to the strongest market for the paintings.

Next Day Air Service Case Study

1. Prepare a brief management summary on the technical essential aspects of the Internet and the World Wide Web and how they work. Remember, the audience is not technical. He is confused about the relationship between the World Wide Web and the Internet and often states that they are the same. Please be sure to explain this in your summary.

   One thing to remember and to emphasize with your students is the point that this question brings out, namely that there is great confusion between what constitutes the Internet and what exactly is the World Wide WEB. The majority of my students are surprised to learn that there is a major difference. The answer is simple, one is the physical layer, hardware nuts & bolts that makes up the highway upon which network traffic will flow. The other (WWW) is but one, albeit now the largest, applications that are available to run over the Internet.

   The Internet actually began without the WWW. It was a bit level, text based network that evolved in a largely DOS based world. For the most part, from its inception it required the TCP/IP protocol suite to be running on the source and destination hosts that were interoperating as we use to refer to it back in those days. As WINDOWs and the graphical user interface evolved so did the ways that we used the Internet.

   In the early 90's after a few years of using, testing and refining several other GUI applications to support Internetworking, the WWW application became standardized along with a few new protocols which were added to the TCP/IP protocol suite. These included HyperText Transfer Protocol now known simply as HTTP and Domain Name Server, now simply known as DNS.

2. President Coone is particularly intrigued with the potential of the Internet, but he and the other members of management are not exactly sure what or how NDAS can use them to improve its competitive edge. Present some alternatives. President Coone reminds you that NDAS expects to enlarge its scope in the international market. Plans call for first offerings to be services to Britain, France, and Germany, with later expansion to South America. President Coone wants you to involve Bob Jones in your work on the Internet.

The Internet is global these days. Carrier access providers, known as ISPs, can provide a company like NDAS with a number of network transport options to connect each of their sites, both domestic and international to the Internet. Once connected there are many applications that NDAS could consider. NDAS could put in place an Intranet at their headquarters. Each of the other sites could access any of t he applications running on the Intranet via the Internet. NDAS could for example have a standard Email application system and make this available to everyone in the company. NDAS could develop a WEB Site for its employees as well as its customers and suppliers to access via the Internet. It is common these days for companies to do this. The type of WEB Site applications typically can run from simple apps like providing essential information about the company to having elaborate back end database applications supporting things like order entry and making electronic payments.

The Marketing departments of companies these days are involved in the development of corporate WEB Sites because of the tremendous reach that a WEB Site can have in the marketplace. As such, Bob Jones' department should be consulted and have representation in the WEB Site development process. The image projected by the quality of the WEB Site will be a critical factor to its success. Bob Jones' department has the expertise to lend in making sure that the WEB Site adequately represents the NDAS corporate image.

3 . With the updates planned for the network , President Coone wonders what other benefits could be derived from the network . One that he particularly is intrigued by is video-conferencing. Explain to him in a memo how the video-conferencing could be beneficial.

The students should create a memo addressed to President Coone that includes some of these main benefits of video-conferencing:

Decreased travel time
Decreased travel expenditures
Better communication (relative to phone)

Additional Content

Teaching Notes

I usually spend 3 hours of class time on this chapter.
I also include hands-on labs on (1) HTML (using Microsoft Word, Front Page, or Dreamweaver) to ensure that all students can create their own web pages and (2) FTP (using both a graphic-interface FTP application and command line FTP access) to ensure that students can transfer files. Sometimes I include a hands-on Web and e-mail lab as well.

I have several goals when I teach this chapter. First, I want students to get a sense of the history of the Internet beyond what they already know. Most of my students think the Internet has always been there. The "traditional" history given in Introduction to Computing courses usually mentions that the Internet started in the late 1960s. This is true, but can be misleading; it implies the Internet has always been an important network. I try to show how small it was at first and illustrate that that it was only one of several possible networks that could have "won." I also try to impress upon them the extremely rapid growth in the past few years. You might want to update the timeline with more recent statistics on the number of Internet users. See www.boardwatch.com. It is useful to explain that the Internet was not originally designed for commercial activities, and that this lack of a business intent carries over into some of the more difficult aspects of traffic management and control in today's environment.

I have two goals for the Internet applications section. First, I want students to become familiar with the Web, SMTP, FTP, and telnet, although for most students this is remedial. Starting with this material, however, helps students to understand the importance and relevance of the course – everyone wants to learn more about the Internet.

The Internet applications discussion is also a good place to explain exactly what is meant by standards and layers from Chapter 1. The HTTP/SMTP standards help students understand why we need standards and *most importantly* that there are standards at all layers in the network model. This underscores the concept that each layer is distinct and has a packet within a packet within a packet, something I have always found that students have difficulty understanding. In my opinion, this concept is more important than having them memorize the contents and format of each type of packet, although I require them to be able to explain the parts of the packet and what each does.

Electronic commerce is an important topic. Most students want to learn about it, and many have been exposed to it in prior classes. I cover enough to help them sort out what is going on the Web with respect to the use of the Internet to operate the back end of businesses using electronic commerce. I also try to link the material to their marketing or economics courses. We discuss aspects of purchasing goods over the internet, and I also ask them if they have purchased anything over the web, used instant messaging or else used desktop videoteleconferencing. Most students have done so, and they are interested in this chapter because it begins their understanding of the nuts and bolts of how web pages and web site forms might be transmitted over networks.

War Stories

Electronic Commerce and Prices
(Objective: Illustrate the implications of electronic commerce for today's businesses; The potential is immense).

A friend of mine recently decided to get a car loan for a new car. After checking out Edmund's (www.edmunds.com) for information, he clicked on the link to a car loan firm. The loan quote was 7.70%. He then called his bank and USAA (a large financial organization well known for offering cheap loans to U.S. veterans). Neither could match the loan rate, although USAA came the closet at 7.85%. Neither would match the Internet rate, even though he had extensive ties to both. It turns out the company offering the low rates on the Internet was actually his bank, doing business under a different name. Electronic commerce has vast implications for business, and this chapter is about the technical underpinnings of how this information moves around the internet.

E-mail
I usually describe my first experiences with e-mail, which were before the days of the Internet. You may also have some good e-mail war stories. The objective is to reinforce the changes in technologies; the Internet hasn't always been dominant. Sometimes I cite an alternative e-mail technology, the US Veterans Affairs (VA) FORUM, the VA's national electronic mail system. Electronic discussions, conferences, distribution of VA directives, news, and computer programs are its primary functions. FORUM disseminates information across any communications medium and also hosts several national databases. Because VA FORUM works according to e-mail threads, it has been extensively used to document the process of software development in the VA health care system.

Protocol Analysis: Capturing Packets

This lab should take 1 – 1.5 hours. Level: intermediate

Objectives

This lab will introduce you to "packet sniffing," a method by which we can capture packets being sent between computers as they communicate. As a network administrator you can use this method to help evaluate the performance of your network by identifying bottlenecks and slower performing servers or sections of your network. You can also use it to check the security of your network. As a graphic demonstration of this, you will configure an FTP server and observe the login packet interchange. You will see that each communication may consist of several packets that are exchanged between the two computers and you will see the potential for security leaks and how to gauge potential abuse of the network by users.

Overview & Prerequisites

You will first install a program called Wireshark. This is an open source application freely available on the Internet that allows you to capture packets as they appear at the network adaptor card. This means that you will be able to see all header information on the packet from each of the OSI layers. (Normally these headers are stripped off so that the only portion remaining is the data payload.) You will use the software to view complete packets and locate each layer's header, from the physical layer to the application layer. Doing so will help you to better understand network traffic and identify things that are "out of order." Using this program you will:

1) Analyze simple protocols and learn about the software interface and the information it contains;
2) Observe, analyze and reconstruct specific packet interchanges between a computer and a server; and
3) Monitor the login process to an FTP server. This will include searching for the login information in the Wireshark output.

For the first two parts of this lab, you will need a single computer with an Internet connection. For the last part, you will need two computers, one of which should have an active FTP server loaded on it. Instructions are provided in part 3 for setting up an FTP server on one computer and connecting to it from a second computer using an FTP client.

Procedure

To obtain the software that you will use for this lab, go to www.wireshark.org and download it to your workstation. Once downloaded, you can install the software and accept all defaults. The program includes a helper program called WinPCap, which will install after Wireshark is installed.

Part 1: Analyzing simple protocols

After you have installed Wireshark, start the program. The initial screen will resemble Figure 1. Notice that your local interface is listed (if you have multiple interfaces, you may see more than one entry; the names may vary). You can click the interface and press "Start" to begin packet capture.

Written by Michael A. Chilton, Ph.D., Associate Professor of MIS at Kansas State University. Updated by Faiz Currim, Ph.D..

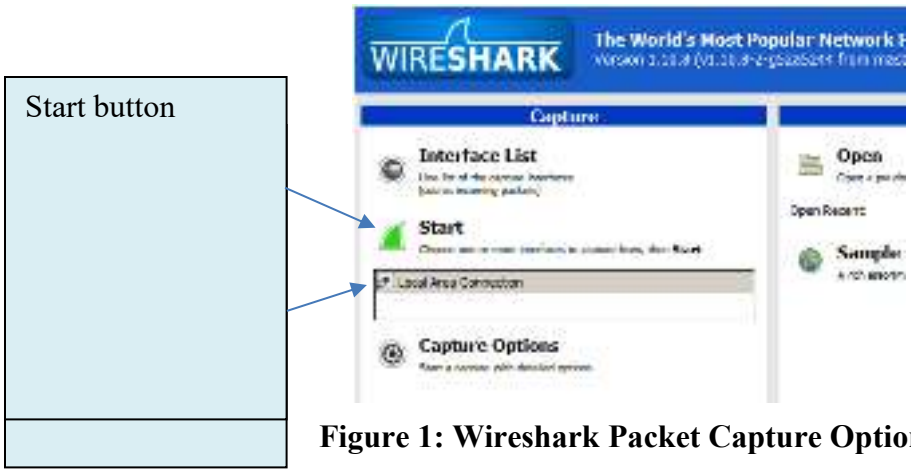


Figure 1: Wireshark Packet Capture Options

Below the menu, the capture window is divided into three distinct areas. The top is a listing of all packets received—the packet list pane; the middle provides the details of a packet selected in the packet list pane and is called the packet details pane; and the bottom, called the packet bytes pane, shows the hexadecimal details of the selected packet and will highlight its (selected) fields. Figure 2 illustrates this and shows some captured packets.

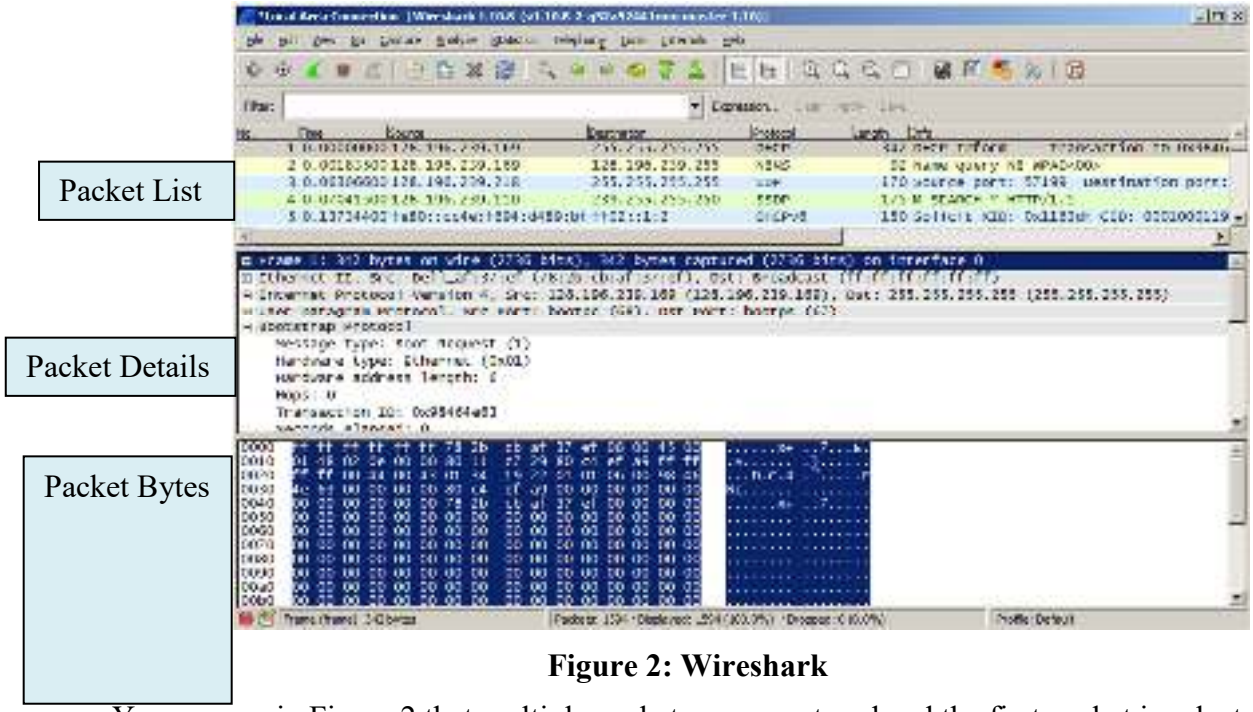
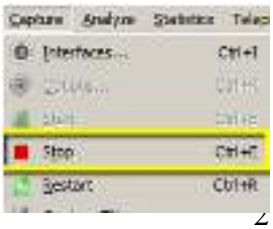


Figure 2: Wireshark

You can see in Figure 2 that multiple packets were captured and the first packet is selected in the packet list pane. In the packet details pane, you can see the Ethernet frame header, the IP header, the UDP header and finally the data payload, which indicates that this is a Bootstrap Protocol packet. The packet byte pane shows the hexadecimal and ASCII equivalent of each packet at the bottom of the window. Selecting a field in the packet details pane will highlight the hex and ASCII portions of the packet in the packet byte pane.

Go ahead and start a capture session and after receiving a few packets, stop the packet capture (from the Wireshark menu, select the "Capture" menu item, and choose the "Stop" command from the drop-down menu).



Find a TCP packet in the packet list pane and select it. In the packet details pane, click on the "+" next to the word "Frame." When this part of the packet opens, you will see some summary information that Wireshark logs about every packet that it captures. Now open each subsequent section of the packet beginning with "Ethernet II." You should be able to find the portions of each packet corresponding to figures 3a through 3c within the packet details section (though the sizes of each section may not always be apparent without closer examination).

Preamble	Start of Frame	Destination Address	Source Address	Type	Data	FCS	Flag
7 bytes	1 byte	6 bytes	6 bytes	2 bytes	46 - 1500 bytes	4 bytes	8 bytes

Figure 3a: An Ethernet II Frame Layout

Version Number	Header Length	Service Field	Total Length	ID	Flags	Fragment Offset	Time to Live	Next Protocol	Header Checksum	Source IP Address	Destination IP Address	Data
4 bits	4 bits	8 bits	16 bits	16 bits	3 bits	13 bits	8 bits	8 bits	16 bits	32 bits	32 bits	Variable

Figure 3b: The IP Header Layout

Source Port	Destination Port	Sequence Number	ACK Number	Header Length	Unused	Flags	Window Size	Header Checksum	Urgent Pointer	Options	Data
16 bits	16 bits	32 bits	32 bits	4 bits	3 bits	9 bits	16 bits	16 bits	16 bits	32 bits	Variable

Figure 3c: The TCP Header Layout

Figure 3a includes 20 bytes that are processed in the hardware and will not be seen in the packet details pane. These are the preamble (7 bytes), the Start of Frame (1 byte), the Frame Check Sequence (FCS, 4 bytes), and the final Flag (8 bytes).

Part 2: Finding specific packet sequences

For this part you need a workstation that is connected to the Internet and one that receives its IP address from a DHCP server. You should have Wireshark installed on your workstation from part 1. In step 1 you will observe the packets required to make and break a connection.

Step 1 Observing a TCP connection

1) Ensure that your capture options are set as before and begin another capture session.
2) After the capture session has begun, open a web browser on your workstation, allow the web page to finish loading, and then stop the packet capture session.
3) Look for the first three TCP packets in the packet list pane. TCP packets have a green background color (depending on your settings) and are easily recognized.

These three packets should be listed as [SYN], [SYN, ACK] and [ACK]. This 3-packet interchange builds a connection between two computers. You should notice that the destination port for the [SYN] packet is 80, indicating a web request. The second two packets should provide you with a sequence/acknowledgement analysis.

Step 2 Observing a DNS request/response

1) Ensure that your capture options are set as before and begin a fresh Wireshark capture session. You can discard the previous session or save it to a file.

2) Begin a Command Prompt window. Next, to release the existing IP address, enter the `ipconfig /release` command at the command prompt. See Figure 4. (Note: if your computer has IPv6 configured, you will see the configured IPv6 address; you can release these using the `ipconfig /release6` command.)

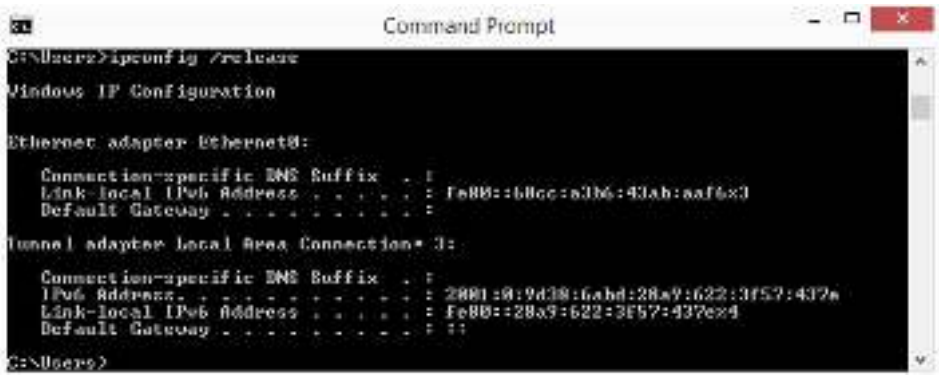


Figure 4: Releasing a DHCP IP Address Lease

3) As soon as you see that your IP address was released (shown as empty or 0.0.0.0, depending on your system) enter the `ipconfig /renew` command at the command prompt. See Figure 5.

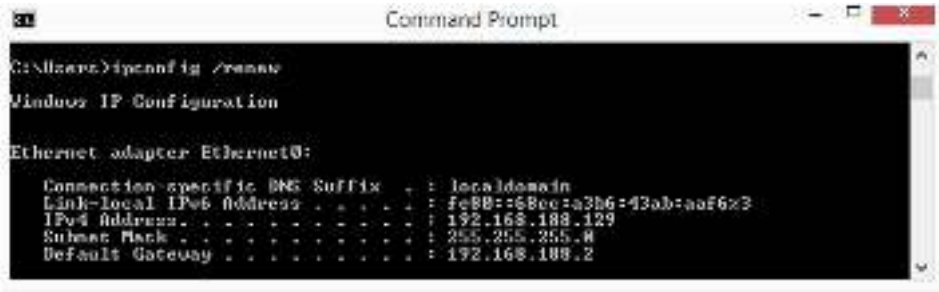


Figure 5: Renewing a DHCP IP Address Lease

4) Wait until the renewal process has completed (you receive an IP address). Then, stop the packet capture in Wireshark. Next, click on the column in the Packet List pane marked, "Protocol." This will sort the entries in order of protocol.
5) Locate the DHCP packets and select the first one. (There should be 5.)

The first of these packets is from your computer to the DHCP server telling it to release the lease on your IP address. The next 4 packets renew that lease. Note that the source address on the "DHCP Discover" and "DHCP Request" packets is 0.0.0.0. This indicates that your computer does not actually use its new IP address until the interchange has completed. Also note that the destination address in each of the 4 packets is a broadcast address[1]. It should be obvious to you why the first two packets are broadcasted, but what about the last two? Can you explain this?

[1] You may see a unicast (your IP address) target for the DHCP Offer / ACK from the DHCP server. This may happen if your DHCP Discover request has Option 50 set to a preferred IP address (e.g., your old IP address).

Step 3: Following an HTTP stream

Let's have a closer look at a request/response interchange that requests a web site. Follow these steps to obtain a fresh set of packets:

1) Ensure that your capture options are set as before and begin another capture session. You can discard the previous session or save it to a file.
2) Open Internet Explorer on your workstation, return to Wireshark and begin a packet capture session.
3) Type in a URL and after the page loads, return to Wireshark and stop the packet capture.
4) Find the packet with comments in the "Info" column saying "GET / HTTP/1.1" and select it. Right click this packet and click "Follow TCP stream" from the popup menu. See Figure 6.

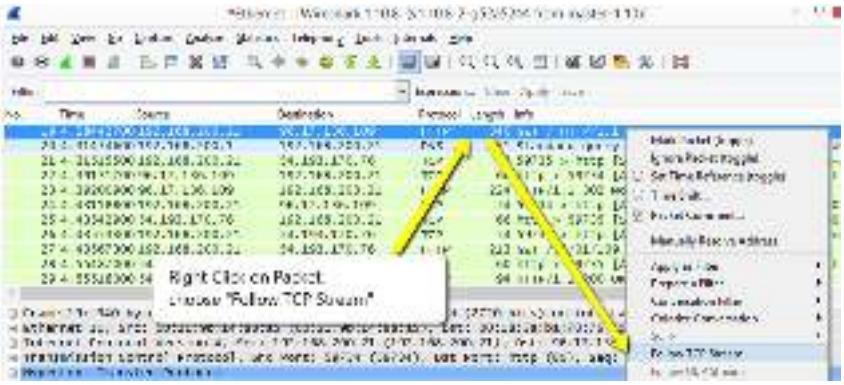


Figure 6: Follow TCP Stream

5) A new window will open with the details of the http exchange. The request and acknowledgements from your workstation are in red, and the responses are in blue and should resemble Figure 7.

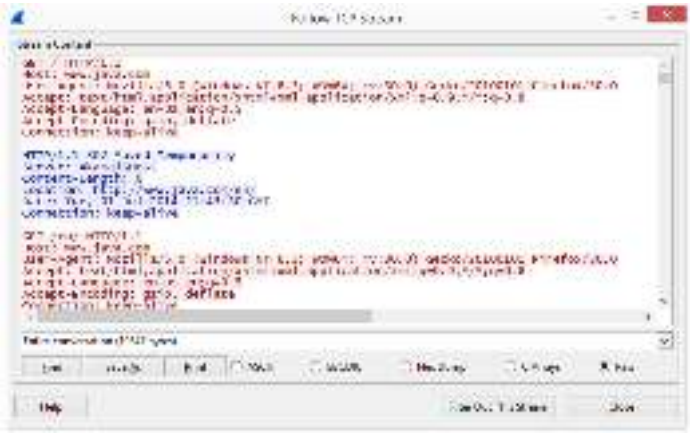


Figure 7: Raw TCP Stream Data

6) At the bottom of this window are some options for saving this file for later reference. Click the "Close" button to return to the main window and you will notice that only the TCP and HTTP packets have been retained, since a filter was created based on your action of following the TCP stream. Now select File > Export > Objects > HTTP. See Figure 8. In the resulting window, find the Hostname you visited (second column; in our case, it was www.java.com) and the content-type corresponding to text/html. Then, click the "Save As" button. Save the file (with a ".html" extension) on your desktop.

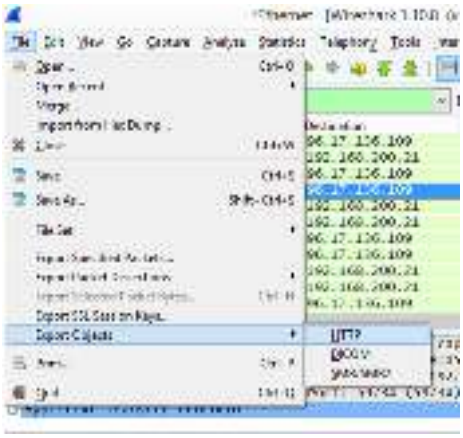


Figure 8: Exporting TCP Stream (HTTP)

7) Minimize all windows and find the file you just saved on the desktop and open it with a web browser. If the web page contains a number of secondary files, such as image, css, or flash files (as many web sites do), what you see won't be very impressive; however, Figure 9 shows http://www.java.com on the left side, while its TCP stream produces the page shown on the right side of the figure. Although you can't see the graphics in the rendered file, you can easily determine its main theme.

Figure 9: Java.com (comparison)

Part 3: Viewing an FTP transfer

We will now look at the file transfer between an FTP client and an FTP server. You will need a second computer on your network capable of providing file transfer services (an FTP

server). The easiest way to set up an FTP server is to download the open source program, Filezilla. It has both a server version that you can use to store files and a client version, which is used to access your server from another computer.

Step 1: Setting up the FTP Server

Download the Filezilla server from http://filezilla-project.org and install it on one computer. You can accept all the defaults for this demonstration, but you will need to create a user and assign a home directory to that user. Make sure you give the user a password but do not enable SSL. For this lab, we chose the username "johndoe" and a password "secret". See Figure 10. *Note: Your firewall may need to be configured to allow connections to FileZilla Server.*

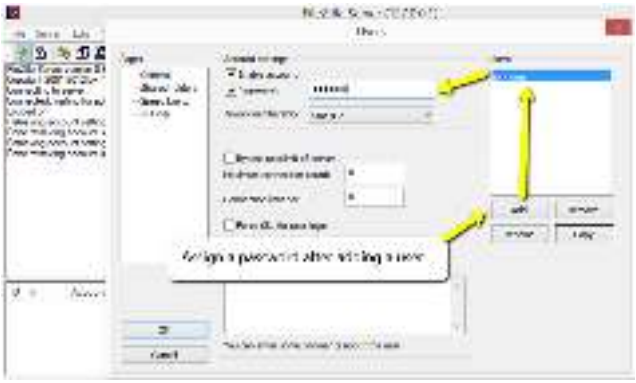


Figure 10: Creating an FTP user in FileZilla

Download the Filezilla client from the same website as above and install it on a second computer. You can accept all the defaults including having the program start after installation.

Step 2: Monitor the FTP login exchange

To see the packet interchange between the two computers, perform the following:

1) Open Wireshark on the client, ensure that your capture options are set as before and begin another capture session.
2) Connect to the FTP server by typing in its IP address, user name and password in the text boxes at the top of the client software, then press "Quickconnect". This is shown in Figure 11.

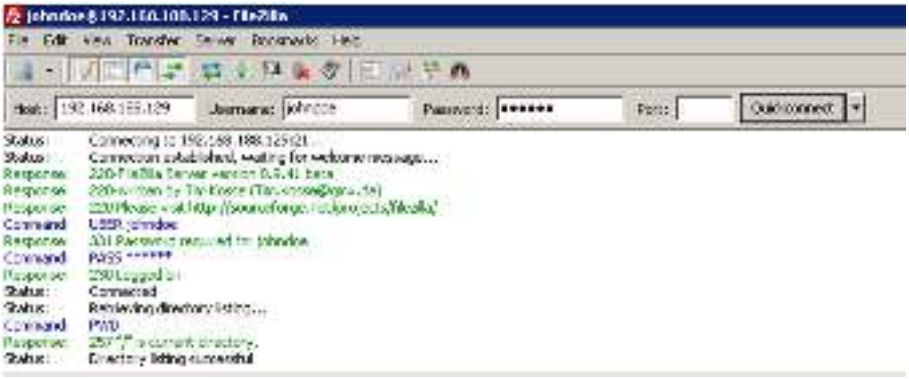


Figure 11: Connecting to the FTP Server

3) Stop the packet capture.

Look for the FTP packets in the Protocol column (or apply a filter to show only ftp protocol packets). In the "Info" column they will say "Request: …" and "Response: …" You should notice that the username and password are displayed for you in this column in clear text. This is shown in Figure 12.

If you have never seen a password revealed in a packet sniffer, it can be a real eye opener. Although we know that FTP servers are inherently not secure, this demonstration should make you think about the security of other types of logins. Try this: if you have a domain controller on your network, try logging on to it from a workstation and sniffing the packets as you do so. Are you able to find the password? (Hopefully not.) Now set up a database server for which the security setting is controlled by the operating system and do the same thing. If the security is not configured correctly, not only will you be able to find the login information (user name and password), but data will be passed in the clear also.

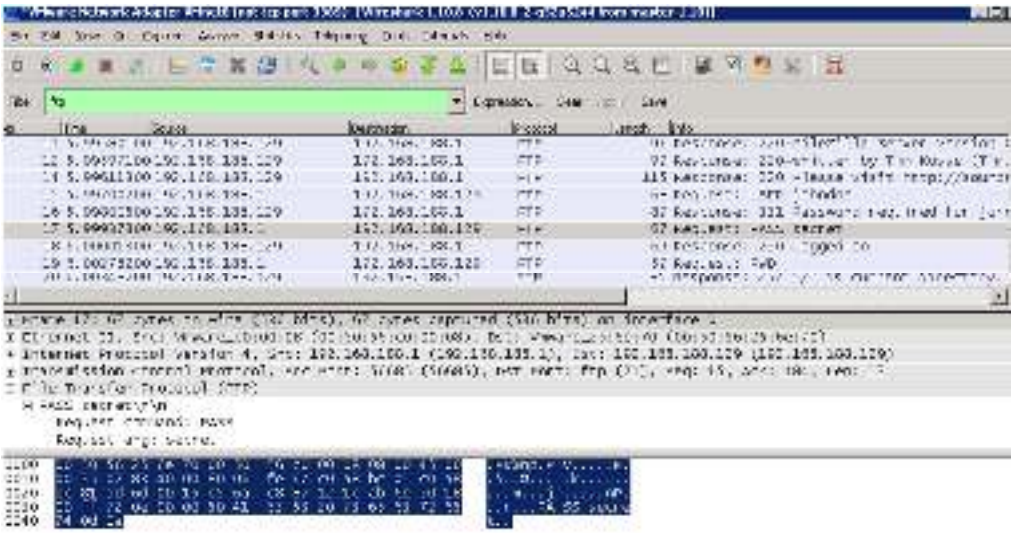


Figure 12: An FTP Login Sequence in Wireshark

Questions

1. Packet sniffing can be a controversial subject. Discuss any issues related to ethics that might arise when an organization monitors the electronic activity of its employees.
2. You looked at packets captured during a web page request. What might this be useful for?
3. Most computers are connected together with switches (rather than hubs). How does this affect the packet capturing process?
4. Discuss how sniffing packets from wireless networks might differ from wired networks. Use the Internet to search for wireless packet sniffers. Where might someone go to sniff wireless packets and possibly obtain some "juicy" information?