CyberCheaterBusters.com

Computer forensics and network security specialists to e-catch them!

Benito Mendoza
Department of Computer Engineering Technology
New York City College of Technology
City University of New York
Brooklyn, NY 11201

Objectives

- Provide an overview of network security
- Examine how an attacker can gain control of a network
- Understand policies and measures to protect the network
- Analyze unsecured data packets
- Introduce computer forensics

Prerequisites

- Knowing the TCP/IP and OSI network models
- Basic understanding of the HTTP protocol
- Basic understanding of the TCP protocol
- Basic knowledge about Wireshark packet sniffer

Vocabulary

- Packet, Network Protocol, TCP/ICP, OSI, HTTP, TCP, packet Sniffing, Hexadecimal

Scenario and Characters

- **Jason**: Works as computer network administrator for an editorial company.
- **Jessica**: Is studying International Business Administration and is Jason's girlfriend.
- **Carly**: Is majoring in International Business Administration and is Jessica's roommate.
- **Andrea**: Is a sociology student and she is Jessica's and Carly's roommate.

It is a Friday night. Jason and Jessica have plans to go to the movies. But Jason is late and caught in traffic. Meanwhile, Jessica is watching TV with her roommates. They are so into the show that Jessica has not realized that she should be ready to go.

"The web is more a social creation than a technical one. I designed it for a social effect— to help people work together— and not as a technical toy. The ultimate goal of the Web is to support and improve our weblike existence in the world. We clump into families, associations, and companies. We develop trust across the miles and distrust around the corner."

Tim Berners-Lee (inventor of the World Wide Web) in (Berners-Lee & Fischetti, 1999)

Part I – The Story of the Company

Jason finally arrived to Jessica's place. He knew that they must leave in five minutes; otherwise they would miss the movie, but, he just couldn't get out of the car; the radio show was very funny.

Jason: Great! First, I was caught by traffic and now by this … radio, reality show.

When the story on the radio ended, he ran upstairs. He entered to the apartment apologizing for been late.

Jason: I'm so sorry; the traffic was crazy across the tunnel, as always.

Jessica: Oops! What time is it? I didn't realize it was time go. We lost track of time watching this TV show.

Jason: Well, it is time to go, Baby! And we are very late. What is it? What is this show about that has you girls very entertained?

Carly: Look, look! This woman was suspicious of her fiancé. The dude is cheating on her. She called a private detective group to get proof. The detectives have been following the dude to this place where he sees another woman.

Jessica: The detectives called their client and she is about to go into the place to bust the dude.

Carly: Look, look! I told you, the dude has been busted.

Jason: This is funny. On the radio, I was listening to a similar story. A woman found some flirting messages between her boyfriend and an ex from high school. She called a radio show for help and advice. She wanted to know if this was something serious. While the woman was on the other line, the host of the radio talk show called the dude telling him that he just won a flower arrangement that he can send to anybody he chooses. The host suggests him to send the flowers to someone special and the dude decides to send the flowers to his ex.

Andrea: So, the dude was busted by the radio show?

Jason: Yes!

Jason: I just hope people at my job are not doing the same thing.

Carly: What? Cyber cheating?

Jason: No, leaving their user IDs and passwords written on a sticky note, placed under their keyboard. That is the way the woman of the radio story found the password to her boyfriend's Facebook; she found those private messages there.

Carly: That was dumb!

Jason: Tell me about it! And it can get much more serious than just getting caught cheating. That's why at my company we spend a lot of resources educating our network users. You would be surprised by the things they do with their authentication information.

Andrea: Is that bad?

Jason: Yes! And you will be scared about things hackers and cybercriminals do to get users information such as passwords and credit card numbers. Sometimes people just give those things away too easy!

Jessica: Really? Like what?

Jason: Hackers, attackers, or intruders sometimes they just go 'phishing', with 'ph' not with 'f'. They ask the users for their passwords or authentication information, sometimes directly---by calls or in person, and sometimes indirectly---through emails or letters. Criminals can even, somehow, persuade the users to divulge confidential information.

Andrea: How come?

Jason: They just pretend to be someone from the company, like a network support specialist, or some other trusted entity.

Andrea: So, they use some kind of social or physiological trick to make the target user cooperate with them?

Jason: Exactly!

Jessica: I've heard that hackers make use of viruses and other nasty programs to get your information, right?

Jason: Yes, they exploit any operating system's vulnerability or the users bad habits to plant viruses, worms, Trojans, spyware, malware or sniffers to collect information or obtain control over the systems.

Jessica: What kind of things can these bugs do in your computer?

Jason: Well, they might track your activities or collect user's ids, passwords, credit cards numbers, etc.

Carly: What do you mean by activities?

Jason: Sniffers can track all the messages or data in and out of your computers. Spyware and adware can look at your browsing activities, like the sites you visit and the products you buy or you are checking. Then, that information can be sold or used to put ads or popups that have products or services like the ones you have been looking at.

Andrea: What do you mean by messages? Like Chat or Facebook messages?

Jason: Sniffers can catch any kind of data going through a network card. So, yes, it is possible to sniff into chat or Facebook messages.

Carly: This is it girls! Remember I've been telling you about making our own business using our combined skills? This is it! With Jason's skills and our background on business and social sciences, we can create a private investigator company to catch cyber cheaters.

Jason: *CyberCheatersBusters.co:* computer forensics and network security specialists to e-catch them!

Jessica: I like that! It's catchy!

Questions

1. From the network administrator perspective, what is network security?
2. What is Social Engineering?
3. What is a denial of service attack and how it is initiated?
4. What is network flooding?

Part II – User's Education

What do hackers do? How do they gain access or control of a network? What does the network administrator need to know to protect the network?

"Jason, you have to train us so that we can help you with the cases," said Carly.

"Of course," replied Jason. "Educating the users is the only way to fight cyber-criminals. I think it is important for our company that every one of us is aware of what they do, some of their tricks might become handy for us," Jason concluded.

Phishing

"I'm interested in the social tricks cyber-criminals use. I'm going to start by learning more about 'phishing'." said Andrea.

"Good idea! You can share what you learned with rest of the group," replied Jason.

The term *Phishing* typically refers to an attempt to obtain information such as usernames, passwords, and credit card details using a fake e-mail or instant message. A phishing attack normally starts by

sending an e-mail that masquerades as a trustworthy entity. The e-mail often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate site (Beasley, 2009). Figure 1 presents an example of a phishing e-mail.

Phishing exploits poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures (Jøsang & Alzomai, 2007).

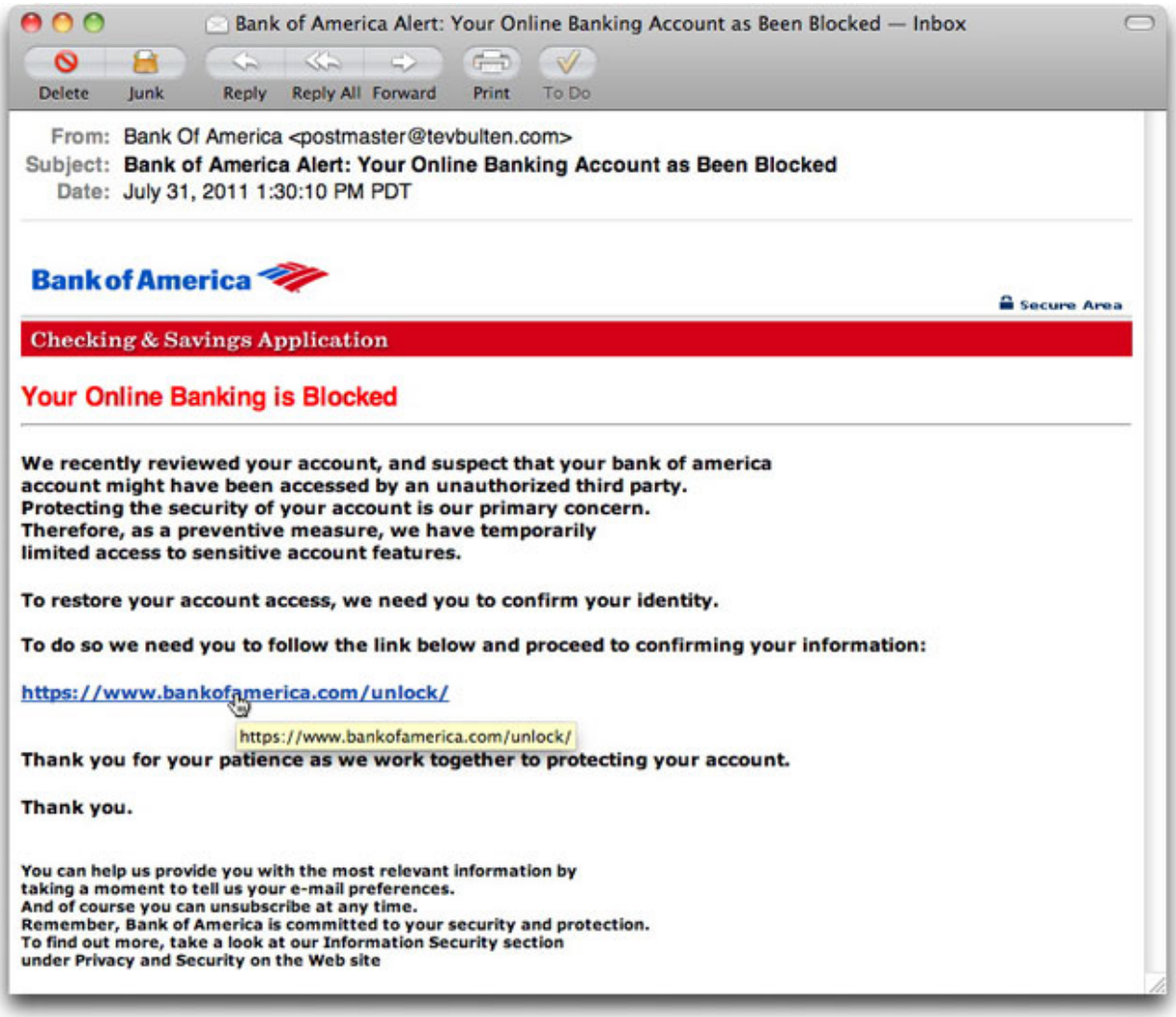

Figure 1. A phishing attack example. A fake email obtained from (Goodman, 2012)

Viruses and Worms

"Well, I will search more about viruses and worms," said Jessica.

"Good idea, Baby! You too can share with us what you learned," replied Jason.

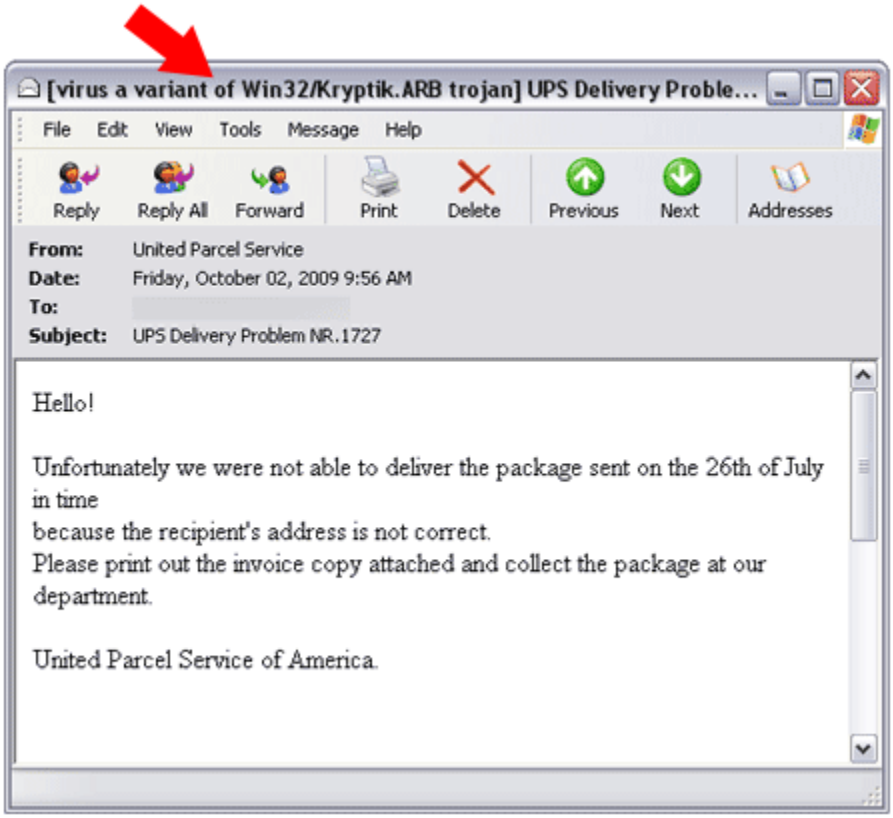

Figure 2. Fake UPS e-mail containing a virus and caught by an antivirus software. *From*: United Parcel Service. *Subject*: UPS Delivery Problem NR.1727. *Attachment*: File_UPS_N1efac8.zip (Hoff, 2012).

A *virus* is a malicious piece of software that when run on your machine might open a backdoor to the machine, start a program that attacks other applications and more (Beasley, 2009). Problems caused by viruses include:

- annoyance
- clogging up the mail server
- denial of service
- data loss
- open holes for others to access your machine
- attack other machines or networks on demand

Today, most viruses are exchanged via attachments via email but hackers can exploit system software vulnerabilities to plant some viruses. For example, Figure 2 shows an example of an email carrying a virus as an attachment. If the attachment is opened then the user's computer could possibly become infected.

How to avoid being infected by a virus? Do not open e-mail attachments if:

- You don't know the sender.
- You know the sender, but his/her name comes in a very long list of names
- You know the sender but he/she is asking you to try something they wouldn't ask for
- You receive a piece of software, audio, video that you would like but it is not from reputable source

Passwords

"I'm intrigued, I will look for other things cyber-criminals do to steal the user's log in information," said Carly continuing. "Also I will check for guidelines to create strong passwords… I know Jason, I will share this with the group," Concluded Carly with a joking tone and a smile on her face.

"Great Carly! You can also check about packet sniffing," Jason replied smiling.

What to do	Example
Start with a sentence or two.	Complex passwords are safer.
Remove the spaces between the words in the sentence.	Complexpasswordsaresafer.
Turn words into shorthand or intentionally misspell a word.	ComplekspasswordsRsafer.
Add length with numbers. Put numbers that are meaningful to you after the sentence.	ComplekspasswordsRsafer2011.

Figure 3. A strategy suggested by Microsoft to create a long, complex password (Microsoft, 2012).

If an attacker cannot get the password from the user, the attacker can use password *cracking* for guessing the passwords (Microsoft, 2012). Cyber criminals use sophisticated tools that can rapidly decipher passwords. Avoid creating passwords that use:

- Dictionary words in any language.
- Words spelled backwards, common misspellings, and abbreviations.
- Sequences or repeated characters. Examples: 12345678, 222222, abcdefg, or adjacent letters on your keyboard (qwerty).

- Personal information. Your name, birthday, driver's license, passport number, or similar information.

Password strength is a measure of the effectiveness of a password in resisting guessing and brute-force attacks. Users should use "strong" passwords; "weak" passwords are easy to crack. A strong password is an important protection to help have safer online transactions.

Here are some features that Microsoft recommends to create strong passwords (Microsoft, 2012). Some or all might help protect your online transactions. Figure 3 shows a technique to create a strong password.

- **Length**. Make your passwords long with eight or more characters.
- **Complexity**. Include letters, punctuation, symbols, and numbers. Use the entire keyboard, not just the letters and characters you use or see most often. The greater the variety of characters in your password, the better. However, password hacking software automatically checks for common letter-to-symbol conversions, such as changing "and" to "&" or "to" to "2."
- **Variation**. To keep strong passwords effective, change them often. Set an automatic reminder for yourself to change your passwords on your email, banking, and credit card websites about every three months.
- **Variety**. Don't use the same password for everything. Cybercriminals steal passwords on websites that have very little security, and then they use that same password and user name in more secure environments, such as banking websites.

Packet Sniffing

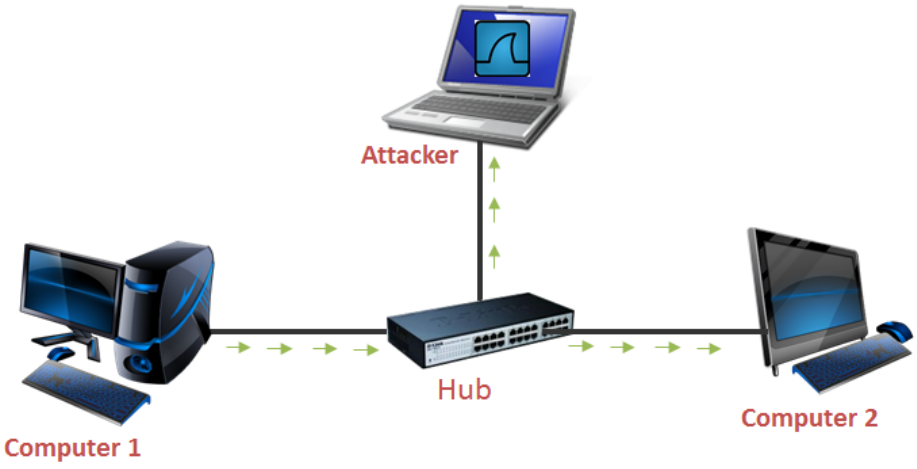

Figure 4. Packet sniffing with a computer connected to a hub. The attacker sees the packets transmitted through the hub.

Another way attackers can obtain a password is by sniffing the network's data packets. This assumes that the attacker can see the network data packets. Packet sniffing is the act of capturing packets of data flowing across a computer network, as shown in Figure 4. The software or device used to do this is

called a packet sniffer, for example Wireshark (Wireshark, 2012). Packet sniffing is to computer networks what wiretapping is to a telephone network.

The attacker will have to insert a device on the network that allows the user to see the data packets. The attacker will watch the data packets until packets from an application such as telnet or FTP passes. Many of these applications pass the user name and password over the network in plain text (unencrypted logins). The way to prevent this is by encrypting the users name and password (Kurose & Ross, 2009). An encrypted alternative to telnet is SSH (Secure Shell). SSL (Secure Socket Layer) is an encryption used by web servers (Beasley, 2009).

Questions

5. List three elements that show the emails in Figure 1 and Figure 2 are faked
6. What is the difference between a computer virus and a worm?
7. What components of a computer's operating and file system a virus can infect?
8. What are software vulnerabilities and how can users protect from them?
9. What is a dictionary attack?
10. Why is packet sniffing easy in a network that uses hubs but not in a network that uses switches?
11. How can users avoid wireless vulnerabilities?

Part III – Sniffing Into Facebook

How can we use a sniffer to see Facebook messages?

"All right!" Carly exclaimed. "I learned about packet sniffers. Let me tell you, a packet sniffer seems to be a complex piece of software. I understand that packet sniffer can monitor messages sent over a network. However, I cannot see how we can use it, for example, to see into Facebook messages." Carly concluded.

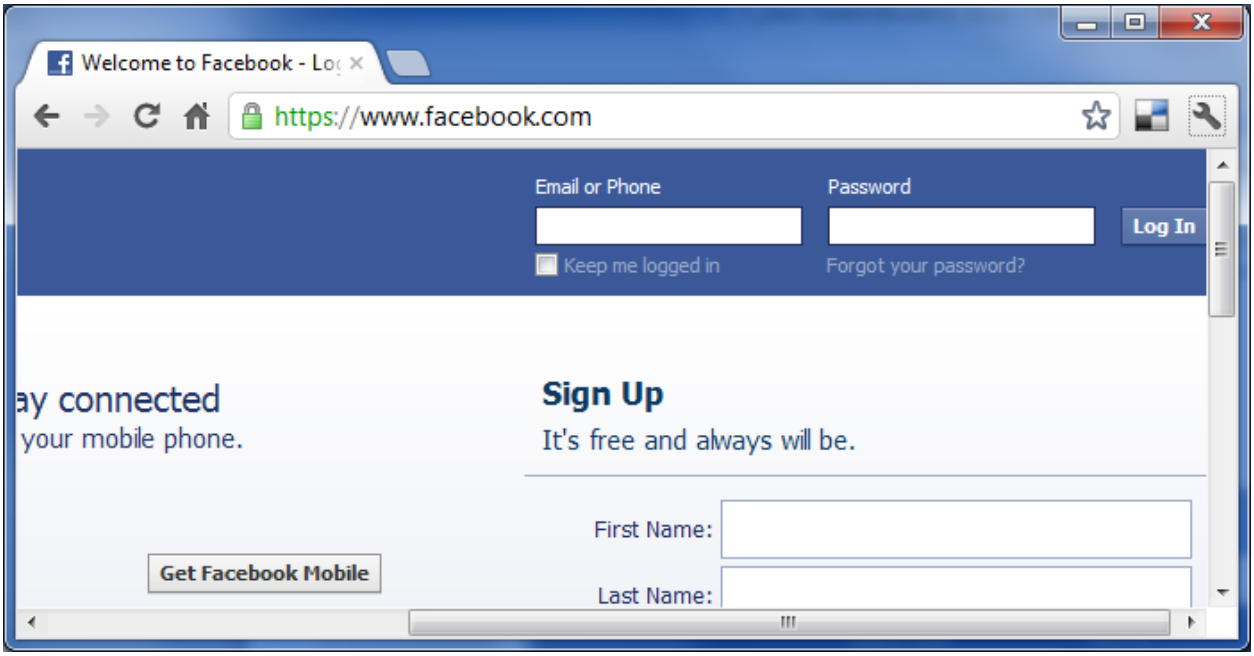

Figure 5. Secure login to Facebook (Facebook, 2012).

A packet sniffer can monitor the network traffic in and out of a computer host. For example, CyberCheatersBusters.com could plant, maybe with the help of a client, a packet sniffer in a target's computer and check all the information sent and received by that computer. Trusted sites, like Facebook, usually have secure connection for the authentication part. For example, Figure 5 shows that Facebook uses the HTTPS (Hypertext Transfer Protocol Secure), which is a combination of the Hypertext Transfer Protocol (HTTP) with the SSL/TLS protocol. HTTPS provides encrypted communication to prevent eavesdropping and to securely identify the web server with which you are actually communicating. That means that even with packet sniffer we couldn't see the user password or other transmitted information. However, once the user logs in into Facebook, regular HTTP is used to access the content on the user account. This means that anything transmitted and received can be seen by a packet sniffer.

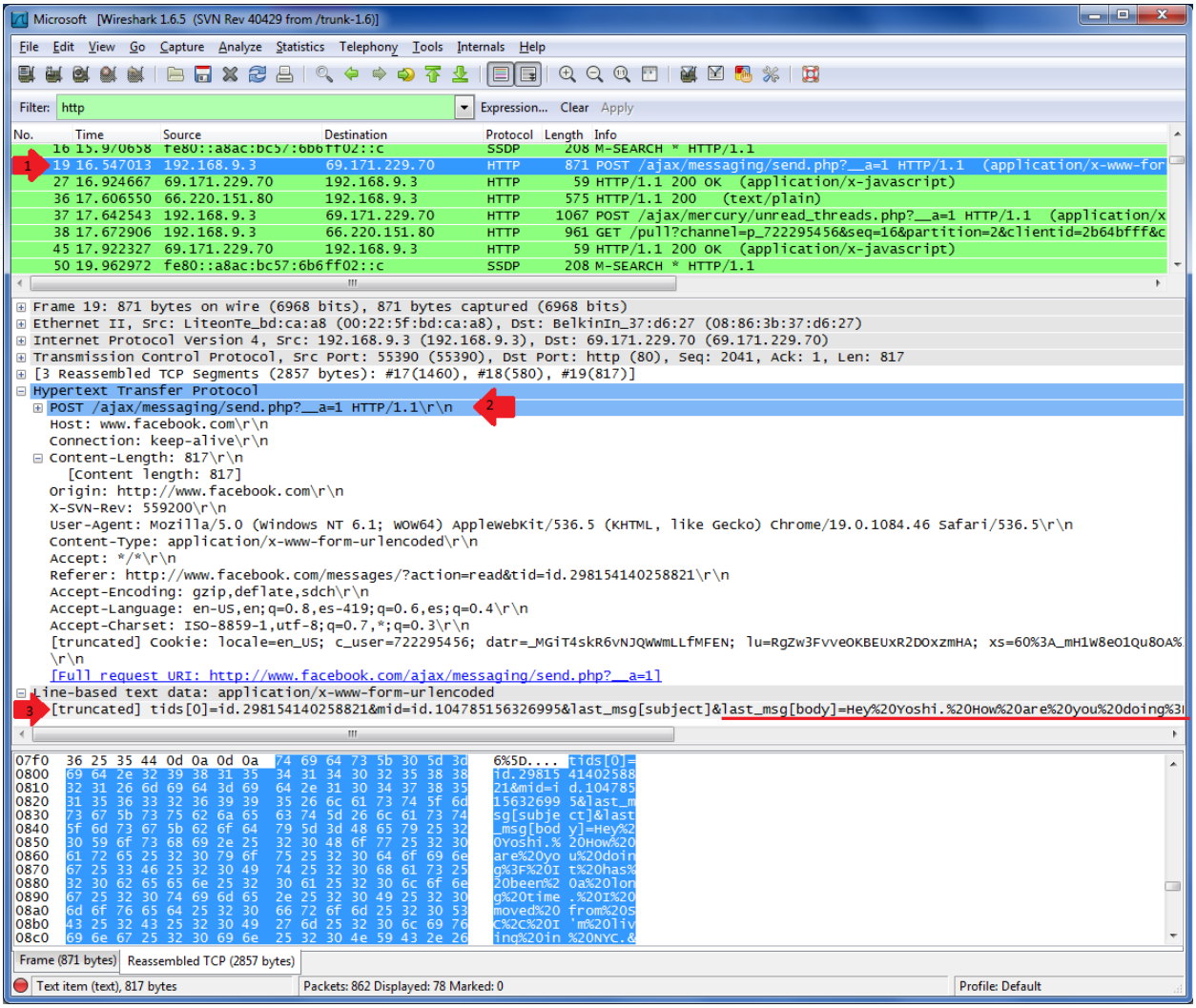

Figure 6. Sniffing into a Facebook message using Wireshark

Figure 6 shows a series of packets captured by Wireshark. The red arrow label with 1 shows packet that is transmitted by the Facebook messaging system, which seems to be a PHP web application. This shows that the POST command of the HTTP protocol is used to send the message. The arrow labeled with 2 shows the details of the HTTP command, including the host and the origin (www.facebook.com). The arrow labeled with 3 partially shows the content of the message, which is underlined with red. The complete message, after the tag [body] is the following:

“Hey%20Yoshi.%20How%20are%20you%20doing%3F%20It%20has%20been%20a%20long%20time.%20I%20moved%20from%20SC.%20I'm%20living%20in%20NYC."

If we replace the characters “%20” with a white space and” %3F” with a question mark, we would have the following:

"Hey Yoshi. How are you doing? It has been a long time. I moved from SC. I'm living in NYC."

Questions

12. What is the Facebook IP address?
13. What is the Transport Layer protocol used by Facebook Messages?
14. What is the HTPP command used to send a Facebook Message?
15. When using SSH or SSL, in what OSI layer is the security implemented?
16. Is it possible to capture messages when using Skype? Explain how and show what you did (screenshots and code for extra credit)?

Part IV – Using a Packet Sniffer as a Computer Forensic Tool

Can we use a packet sniffer to see the images transmitted over the network?

"Packet sniffers are cool!" exclaimed Jessica.

"Yes, I understand that looking at text based messages is possible," said Carly continuing. "But, how about things that are not texts, a picture for example?" Conclude Carly.

"Actually, you can reconstruct pictures too. A packet sniffer looks at everything, no matter what type of data," Jason confirmed.

Byte	1	2	3	4	5	6	7	8	9	10	11
Hex	FF	D8	FF	E0	Skip	Skip	4A	46	49	46	00
Char	ÿ	Ø	ÿ	à	Skip	Skip	J	F	I	F	

Figure 7. Header of the JPEG image format

Images and videos are stored in different types of standardized file formats. An image file may store data in uncompressed, compressed, or vector formats. Before the image can be displayed on a monitor or printed, the data in these files has to be rasterized; that is, converted into a grid of pixels. Once rasterized, each pixel has a number of bits to designate its color.

As with any other kind of data, image files are send on chunks of data or packets over the network. Of course, a packet sniffer can capture all of these chunks of raw data representing an image. The problem is how to find what part of the data transmitted corresponds to the image. For this we will need to know the type or format of the image; that is, we need to know in what file format the original transmitted image has been stored. As a standard, most image files have a header or marker segment that will allow you to determine the image type. For example, Figure 7 shows the header of a JPEG file (Hamilton, 1992), which is probably the most widely used compressed image format.

The JPEG header contains multiple parts that can help us to identify this format easily, as shown in Figure 7. The first things to look for are the two bytes that represent the ***Start Of The Image File***; that is,

the hexadecimal values **FF D8**. In general, this would be enough to know that you have an actual JPEG file. Most of the time, the next two bytes, typically **FF E0**, represent a marker called the ***Application Marker.*** This marker will increase confidence of an image been a JPEG. However, this marker can change depending on the application used to modify or save the image. This market is followed by two blank bytes that should be skipped. The next five bytes specifically identify the application marker. Normally this zero terminated string will be **4A 46 49 46** ("JFIF") and **00** to terminate the string. However, some digital cameras will use **45 78 69 66** ("Exif"). In general, the following sequence of bytes: **FF D8 FF E0 <skip two bytes> 4A 46 49 46 00** will represent the beginning of the file (just remember that the application markers that can vary). The values **FF D9**, not shown on Figure 7, represent the ***End Of Image***.

Figure 8. Mark Zuckerberg's article on Wikipedia

Every time a web page is requested from a web server, all the content is transmitted, including the pictures, for example the picture on a Wikipedia article on Figure 8. A packet sniffer can create logs of all

the pages a user has visited. Then, all of the information seen by the user can be reconstructed. Packet sniffers along with hexadecimal editor are good tools for computer forensics.

For example, Figure 9 shows the packet requesting the Zuckerberg's picture from the Wikipedia page shown in Figure 8. The figure shows, in the green section, that a GET request. The section in the middle shows the HTTP header and the name and type of the picture, we know that it is a JPG image. The lower section shows the raw data of the request in hexadecimal. To retrieve the raw data corresponding to Zuckerberg's picture using Wireshark, we will need to use the option "Analyze->Follow TCP Stream"

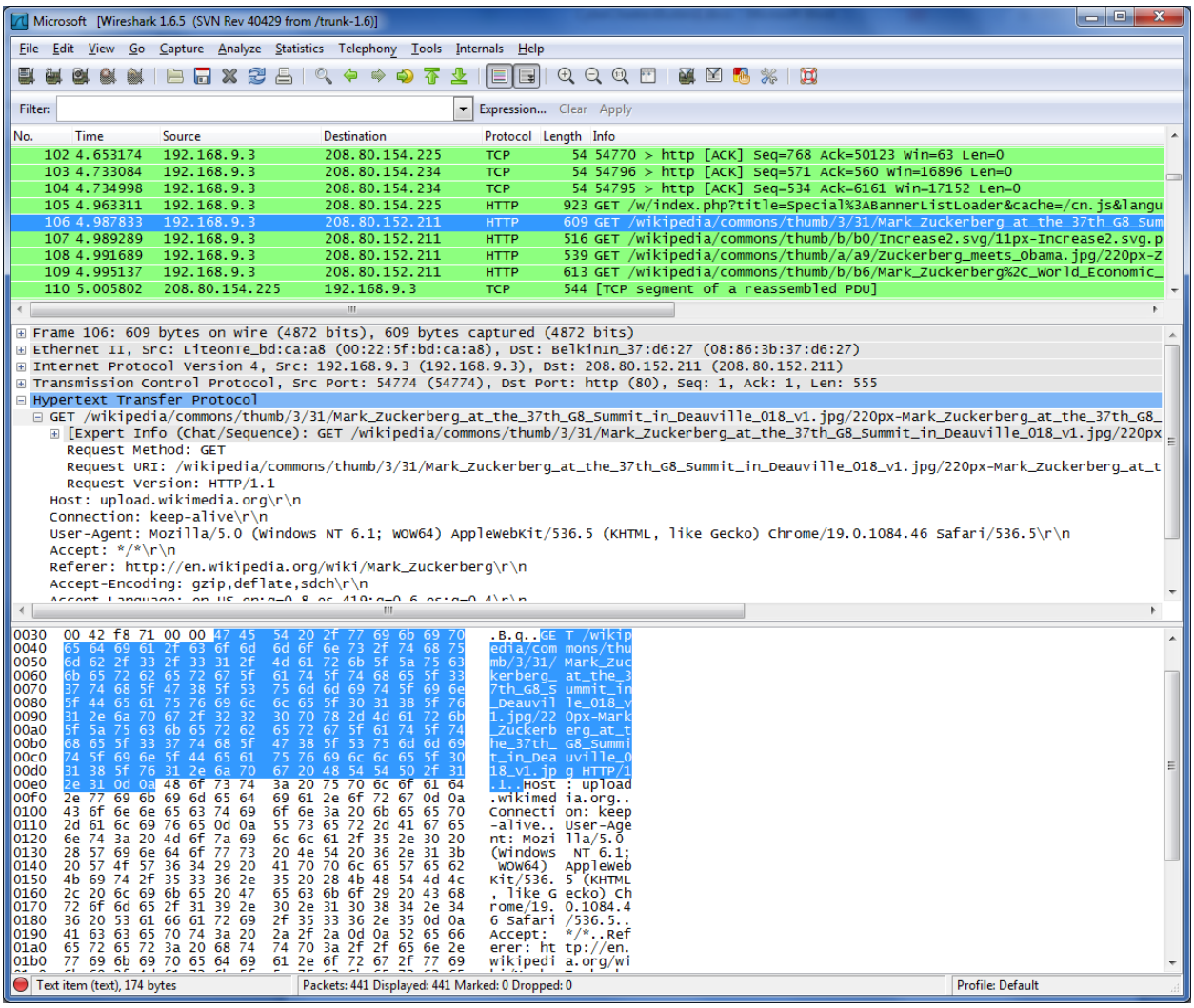

Figure 9. Sniffer showing the GET request of a JPG image from Wikipedia

Figure 10 shows part of the raw data corresponding TCP stream containing the Zuckerberg's picture. We need a hexadecimal editor to extract only the data corresponding to the picture and save it as JPEG file. Figure 11 shows how using a hexadecimal editor called WinHex (AG, 2012), we can easily find the markers that indicate the beginning and, although not shown here, the end of the file. After removing

everything before the markers **FF D8** and after the markers **FF D9**, we can save the raw data as a file with JPG extension to be able to see the corresponding image.

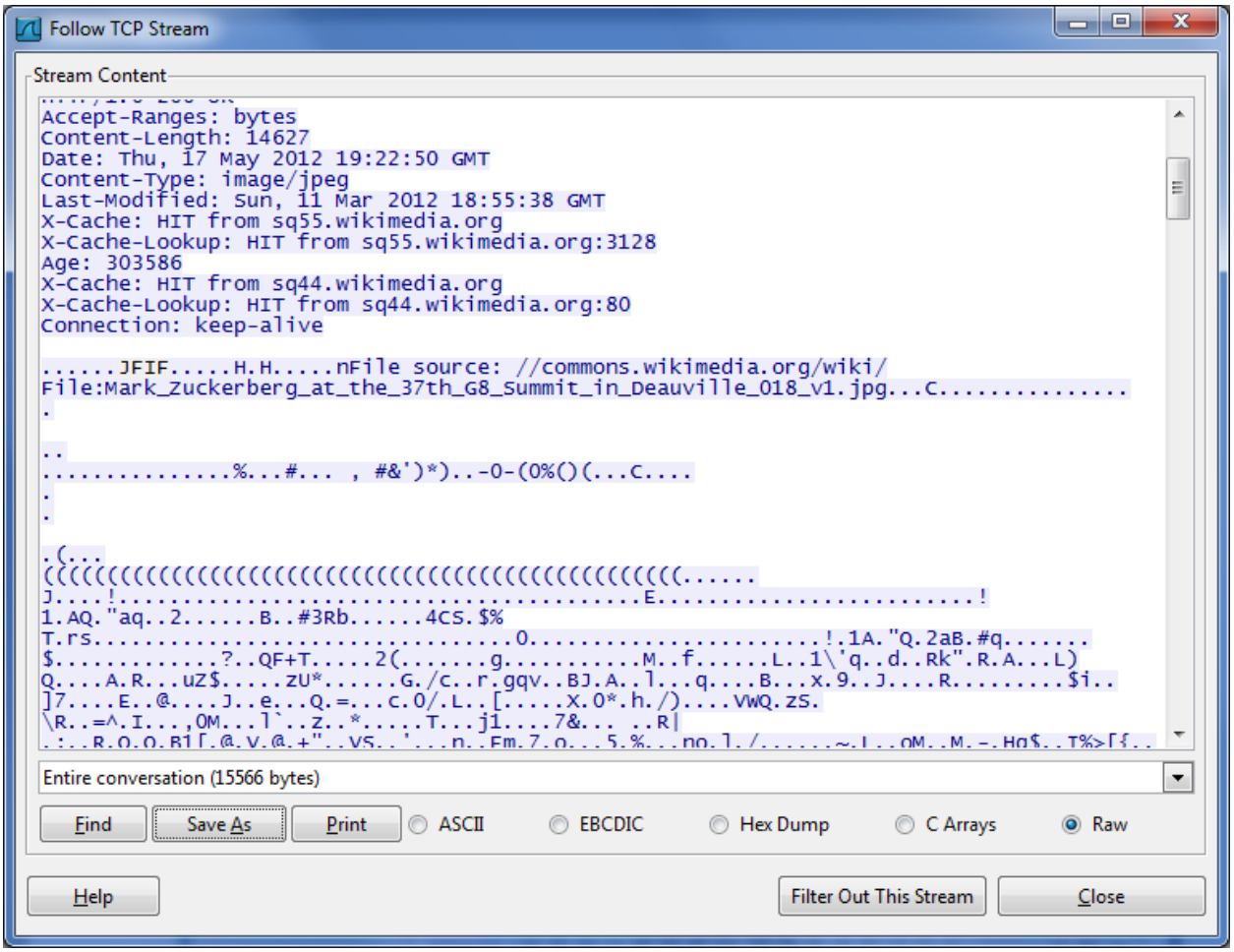

Figure 10. TCP Stream containing a JPEG image from Wikipedia

"All right!" I think we have learned a lot. What we need now is to start doing business; we need our first client!" Jessica exclaimed. "You are right" the others agree.

Questions

17. What would be the markers to look for if the image was a PNG, or a GIF, or a BMP file?
18. From https://sites.google.com/site/mendozaport/, reconstruct the .png picture. Show screenshots and code, if any. (extra credit)
19. What else can "Cybercheaterbusters.com" do by using a packet sniffer to spy on cheaters?
20. What other tools or computer forensic techniques can be used by "Cybercheaterbusters.com"
21. What would be other uses of a packet sniffer as a tool for computer forensics?

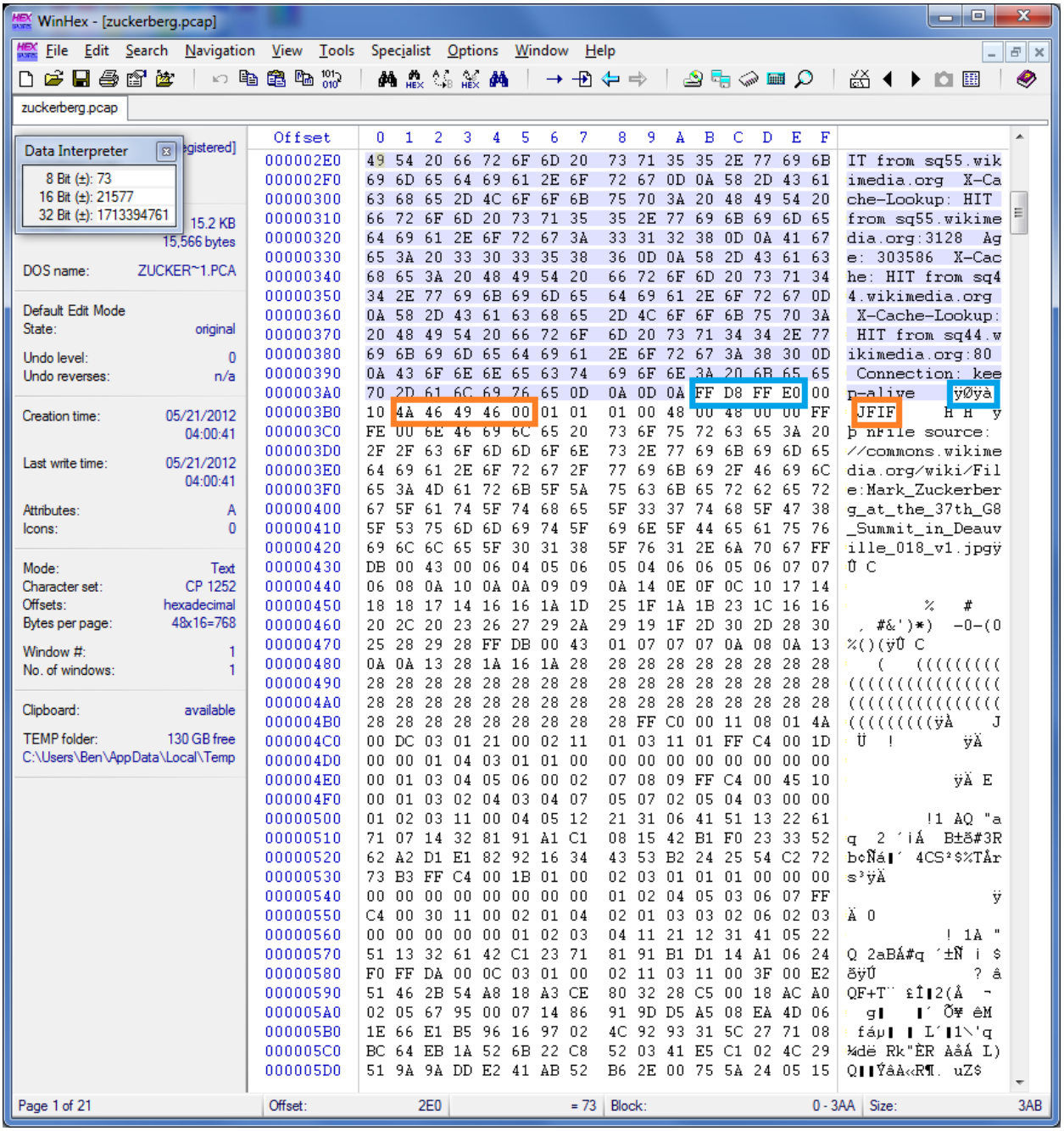

Figure 11. Hexadecimal editor showing the beginning of a JPEG file

Bibliography

AG, X.-W. S. (2012, May 15). *WinHex: Computer Forensics & Data Recovery Software,*. Retrieved from http://www.x-ways.net/winhex/index-m.html

Beasley, J. S. (2009). *Networking* (2nd ed.). Boston, MA, USA: Pearson Educatioin Inc.

Berners-Lee, T., & Fischetti, M. (1999). *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor.* San Francisco, CA, USA: Harper San Francisco.

Facebook. (2012, May 15). *Facebook*. Retrieved from Facebook: https://www.facebook.com

Goodman, D. (2012, May 15). *A Dispatch*. Retrieved from spamwars.com: http://spamwars.com/archives/2011/08/interesting_app.html

Hamilton, E. (1992). *JPEG File Interchange Format.* C-Cube Microsystems. Milpitas, CA 95035: C-Cube Microsystems.

Hoff, L. (2012, May 15). *United Parcel Service Email Trojan*. Retrieved from Lance's Journal: Diary of simple solutions: http://www.lancelhoff.com/united-parcel-service-email-trojan/

Jøsang, A., & Alzomai, M. (2007). Security Usability Principles for Vulnerability Analysis and Risk Assessment. *Proceedings of the Annual Computer Security Applications Conference 2007 (ACSAC'07).*

Kruse, W. G., & Heiser, J. G. (2002). *Computer forensics: incident response essentials.* Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc.

Kurose, J. F., & Ross, K. W. (2009). *Computer Networking: A Top Down Approach* (5th ed.). Addison-Wesley.

Microsoft. (2012, May 15). *Create strong passwords*. Retrieved from Microsoft Safety & Security Center: http://www.microsoft.com/security/online-privacy/passwords-create.aspx

Wireshark. (2012, May 15). *Wireshark*. Retrieved from wireshark.org: http://www.wireshark.org/