Global Information Assurance Certification Paper

GIAC SECURITY ESSENTIALS CERTIFICATION (GSEC)

PRACTICAL ASSIGNMENT

VERSION 1.4B

OPTION #1, RESEARCH PAPER

INSTANT MESSAGE SECURITY – ANALYSIS OF CERULEAN STUDIOS' TRILLIAN APPLICATION

BY

MICHAEL D. MURPHY

JUNE 2003

TABLE OF CONTENTS

I. Abstract

This paper outlines the underlying security risks of Instant Messaging (IM) focusing on an analysis of Cerulean Studios' Trillian application. There are several corporate offerings being released by the major IM providers, but the focus has been on providing a secure application for usage across the corporate Intranet with little to no integration with the public Internet. Cerulean Studios has focused its efforts on developing a secure IM application for usage across the Internet. Trillian is an IM application capable of simultaneously connecting to multiple IM services and is a secure option for corporations to use, allowing employees to collaborate securely via the Internet. Cerulean Studios has developed methods to encrypt IM for AOL and ICQ. This paper will examine the Trillian application in detail, analyze the methods of encryption designed into the application, provide a comparison of the underlying packets transmitted, and provide findings based on the overall research and analysis. Trillian has been widely accepted as a secure tool. This paper supports Cerulean Studios' claim that Trillian provides a secure option for both personal and corporate IM usage. The author of this paper is in no way affiliated with or compensated by Cerulean Studios.

II. Overview of the underlying security risks of Instant Messaging

Instant Messaging has become a low cost method of collaboration within many organizations. It is widely used in corporations across the United States as well as globally with significant evidence that shows usage to be increasing. The findings of Gartner Consulting in an analysis of Reuters, a financial information, technology, and news group, provide significant data points on the trends within IM in the corporate workplace. Reuters contracted Gartner to provide an analysis of the financial industry in the area of IM. The following bullet points highlight some of the key statistics derived in Gartner's analysis:

- 75% of financial institutions view improvements in collaboration as important to critical.
- Gartner predicts that by 2005, IM will be integrated into 50% of applications that directly interact with the customer.
- Over 50% of financial institutions are piloting IM within their organization.
- By 2003, free IM will be found in 70% of enterprises.
- Gartner views free IM as a risk for financial service organizations because of its vulnerabilities.

("Collaborative Technologies", 2002)

The statistics from Gartner consulting are significant in the fact that IM applications are making their way into a majority of corporations throughout the financial industry and the assumption can be made that IM applications are being used equally in other industries.

Because of this, it is important to analyze and understand the implications of IM both in productivity and potential risks to an organization's knowledge capital and network infrastructure. The security of most free IM tools has the potential for major negative impacts within an organization. Corporate employees must understand and embrace the tools that are select by the organization. In many cases individuals understand that most IM applications are not secure, yet sensitive information such as user names, passwords, IP Addresses, etc. is still transmitted. If an organization decides to use an IM application, initiatives must be taken to train employees on what should and should not be sent via the IM tool. Security professionals must ensure users understand the implications of using IM across the public Internet.

In addition to the security impact, the organization must look at the benefits IM can have on communication and collaborative work. IM speeds communications within many organizations as teams are able to collaborate on issues without picking up the phone, drafting and sending an email, or walking over to talk face-to-face with another team member. The ability to link employees across multiple work sites will drive productivity gains while it reduces overall telecommunications costs.

Each organization has a decision to make between security and productivity and must determine if it will embrace or ban IM. In either case, provisions will be required to either enforce the ban or train employees how to best use IM within the organization. In addition to training, security professionals will be expected to fully examine all viable IM options. This examination includes researching the capabilities and limitations of the Trillian application.

A. Instant Message Architecture

The Instant Messaging architecture (Figure 1) is representative of a traditional client/server network. The diagram depicts the basic overall architecture of an IM network. In the diagram, there are three major providers in the IM world: AOL, MSN, and Yahoo. Users have a client application installed locally that communicates with the proprietary servers each vendor manages. These servers are used to facilitate connections with other members of that specific service. When connected, the users can see other users who are actively connected and send them brief text messages. The individual vendor client software is not compatible with other vendors. This has made IM a challenge as a standard means of communications. A user can only connect to the specific vendor server using traditional vendor provided software. Cerulean Studios' Trillian application was created to be a single point of entry into a user's various IM accounts. Using Trillian allows the user to setup and connect to all major providers using a single application. This is a highly advantageous feature, as it allows users to collaborate and communicate through AOL, MSN, and Yahoo simultaneously from a single application, with no impact on functionality. Overall, the secure IM feature available in Trillian makes it more secure than the software provided by the individual vendors.

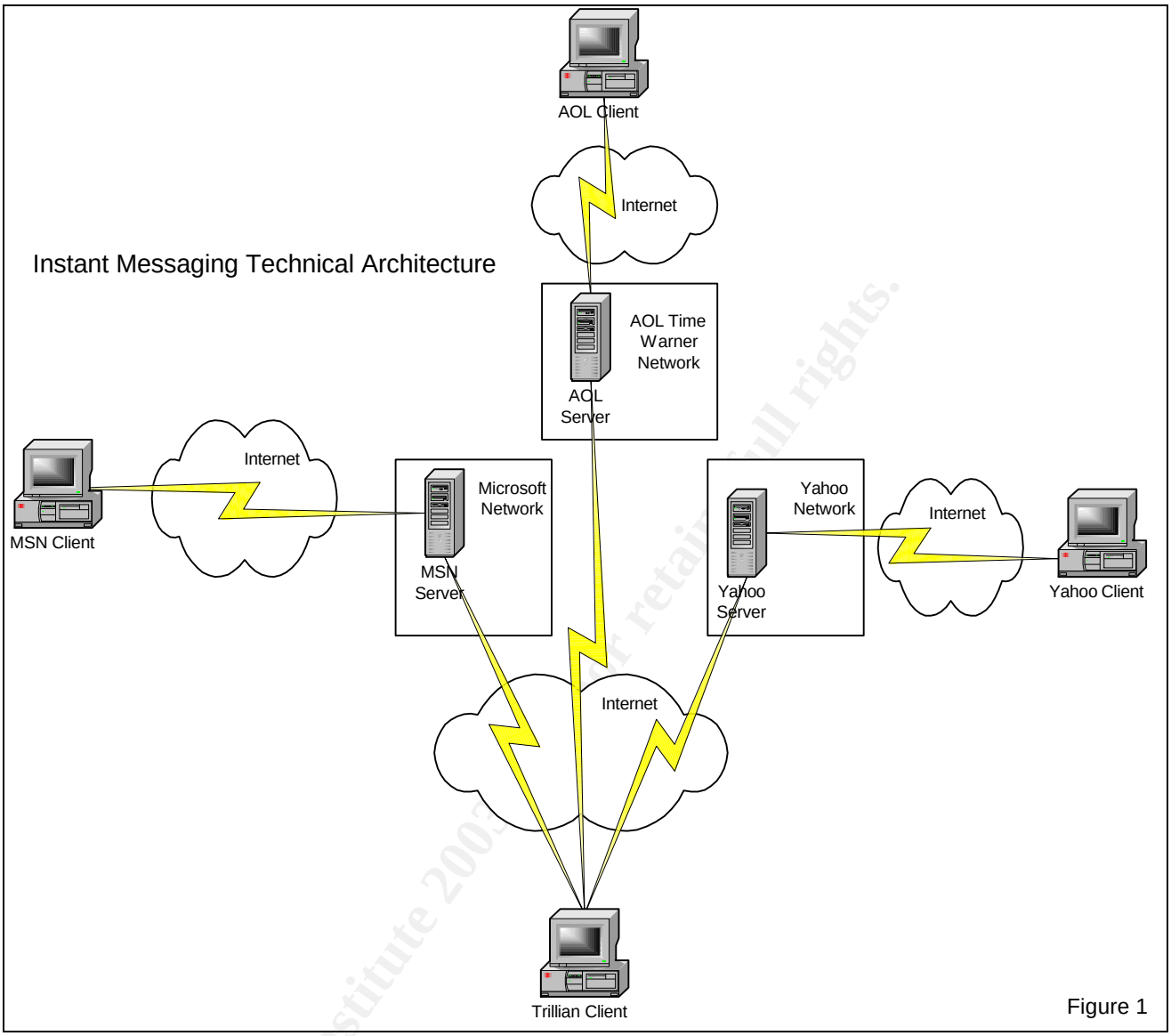


Figure 1

B. Security Limitations

Within the architecture in Figure 1, it is evident that the main security limitations exist in the lack of encryption to mask the data being sent between the client and server. All data is passed in plain text packets that have the potential to be hacked by malicious users. This is a limitation in the main IM providers' client applications. Even so, the ease of use and functionality has increased the demand and implementation of IM tools in the workplace. Cerulean Studios has taken action to mitigate the vendor specific security risks using encryption. In subsequent sections, the encryption incorporated into the Trillian application will be detailed.

C. General Security Options

As displayed in Figure 1, the three top IM providers are AOL, MSN, and Yahoo. Each of these organizations is approaching the security limitation, by providing a corporate solution housed on the corporate Intranet avoiding the potential issues of the public network. This is effective when communications within the organization are focused internally. In situations where employees are distributed outside the corporate infrastructure (i.e. consulting at the client site), this approach will not work without a method to filter IM to and from users on the public Internet. These options have been slow to meet the needs of corporate clients. In the case of IM using AOL, Trillian has risen as an application that can add the necessary security while still providing access to users outside the corporate Intranet.

III. Product Examination – Cerulean Studios' Trillian

Cerulean Studios was founded in May of 1998 by Kevin Kurtz and Scott Werndorfer. The first version of Trillian was released July 1, 2000. The office of Cerulean Studios is located in Connecticut ("Cerulean Studios' Home", 2003). Cerulean Studios promotes and distributes two versions of Trillian at this time. The free version being distributed is version .74. The latest release of Trillian with additional functionality and features is Trillian Pro version 1.0. This version has a small distribution cost, but adds functionality through the addition of plugins. Currently, both versions provide the same level of security.

A. Cerulean Studios' Trillian Version .74

Trillian version .74 is the free version of Trillian provided by Cerulean Studios. The version can be used to integrate AOL, MSN, ICQ, Yahoo, and IRC into one tool. Version .74 tracks conversations using simple text logs. Individual files are saved for each buddy in a user's buddy list. These text files can be accessed easily to review information previously communicated. Trillian is integrated with Windows in a manner where one can drag files into a message window to initiate a file transfer. This version provides secure IM using a combination of the Diffie-Hellman key exchange and 128-bit Blowfish encryption. This encryption capability is limited to AOL and ICQ type messages ("Cerulean Studios' Trillian version", 2003).

B. Cerulean Studios' Trillian Pro Version 1.0

Trillian Pro version 1.0 includes all the features of version .74 with extended capabilities made available via add-on plugins with a cost of $25/person. The architecture currently allows for third party developers to create compatible plugins for Trillian Pro. The plugins available include AccuWeather™, POP-3, World Time Clock, Popup Notifications, News, as well as IM Forwarding. Cerulean Studios states that there are over 100 enhancements to the Trillian Pro version. However, in the area of security via

secure IM, there have not been any enhancements. The other enhancements are not security based features, so overall the two versions are consistent in the level of security they provide to the user ("Cerulean Studios' Trillian Pro", 2003).

IV. Trillian Encryption

Trillian version .74 and 1.0 both support Secure Instant Messaging for AOL and ICQ. This is a key feature of Trillian that must be examined in order to validate whether Trillian truly supports sending secure IM across the public Internet. Trillian uses a combination of the Diffie-Hellman key exchange with 128-bit Blowfish Encryption in order to secure AOL and ICQ forms of messaging. This combination provides Trillian with a basis for sending and receiving Instant Messages securely from one Trillian user to another. Both the source and destination user must use Trillian in order for a secure link to be established.

A. *Diffie-Hellman Key Exchange System*

The Diffie-Hellman key exchange system was publicly introduced in 1976 by Whitfield Diffie and Martin Hellman. It was the first system to use a "public key" or "asymmetrical" key (Palmgren, 2003). An asymmetrical key is unique for each user, but mathematically can be used to derive a common key. The procedures used in the Diffie-Hellman key exchange are provided in Figures 2 - 6. The process is diagramed in the most basic method with integration of how it is used in the Trillian application. The key exchange uses modular mathematics to derive the shared secret key and is depicted by the mathematical operator icon in the process flow in Figure 4. The six steps of the process are as follows:

Step 1 – Generate Public and Private Keys

Both User A and User B create private keys. From their private key they create a public key. At this point all keys are unique, but mathematically will be used to derive a shared key, which is identical for both User A and User B.

Figure 2

Step 2 – Transfer Public Keys

User A transfers his public key to User B. User B transfers his public key to User A. Each user now has their private key and the other user's public key.

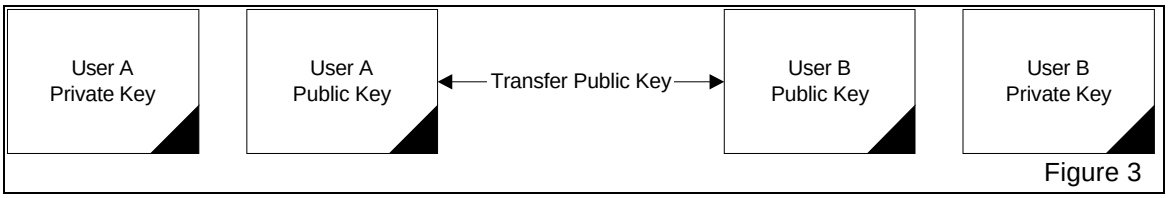


Figure 3

Step 3 – Derive Shared Secret

Each user derives the common shared secret key by running a mathematical operation against their private Key and the other user's public Key. The mathematical operation results in an identical shared secret key which will be used by both users to transfer the symmetrical key which is detailed in Step 4.

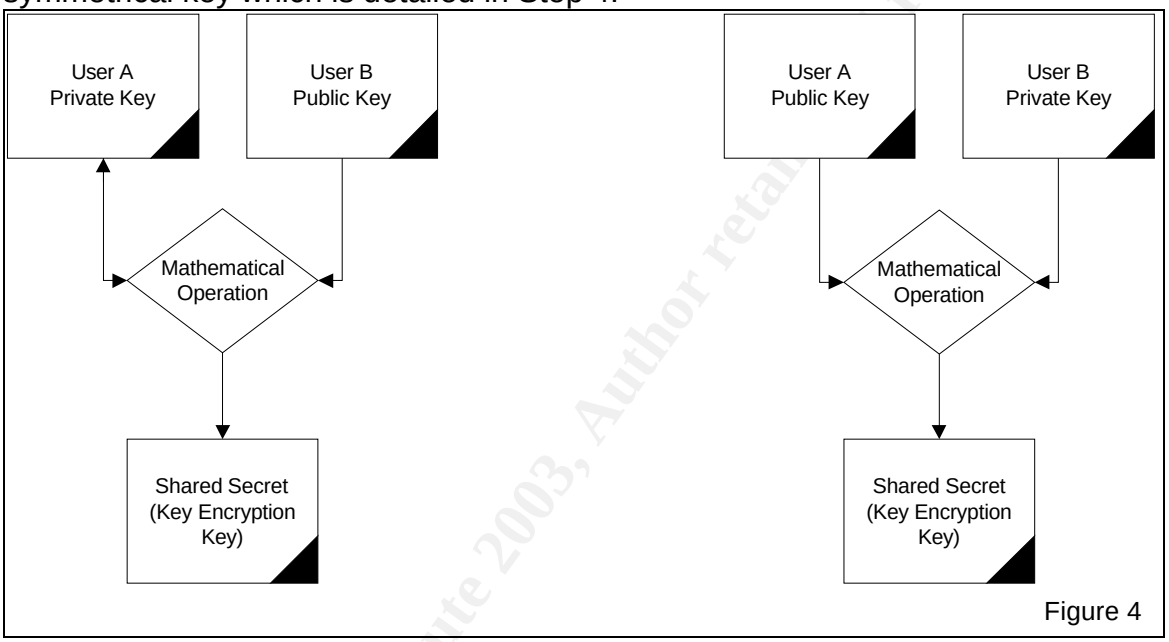


Figure 4

Step 4 – Transfer 128-bit Blowfish Symmetric Key

The symmetrical key is then used to pass data. Using a symmetrical key for the actual data transfer allows for quicker encryption and decryption within the system. Trillian uses 128-bit Blowfish encryption for its symmetrical keys. In this step, the symmetrical key is passed from User A to User B. The shared secret key facilitates the secure transmission of the 128-bit Blowfish symmetric key.

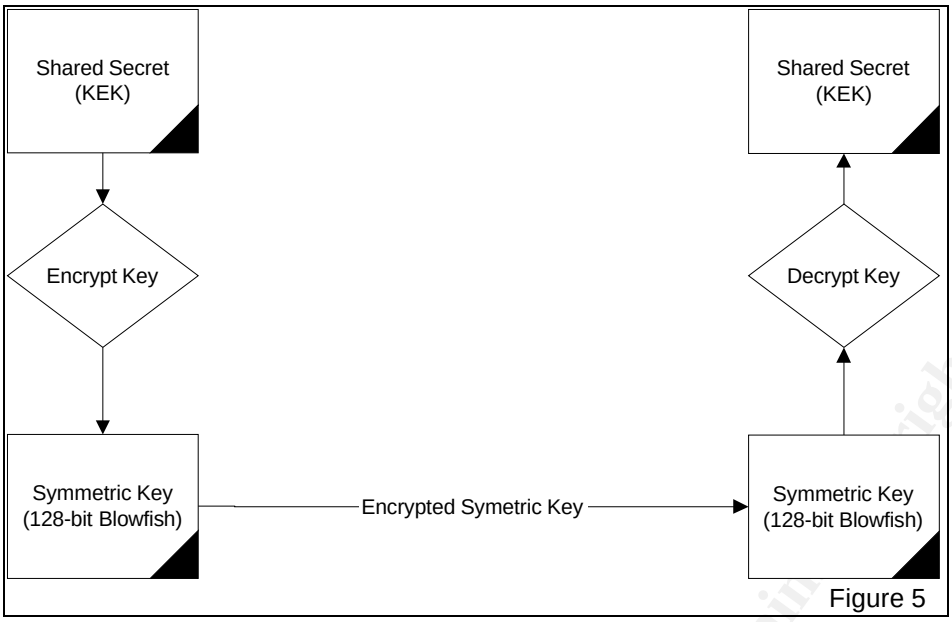


Figure 5

Step 5 – Encrypt Data Using Symmetric Key

At this point a secure 128-bit symmetric key has been passed between User A and User B. The symmetric key is used to encrypt and decrypt all data transmissions between User A and User B.

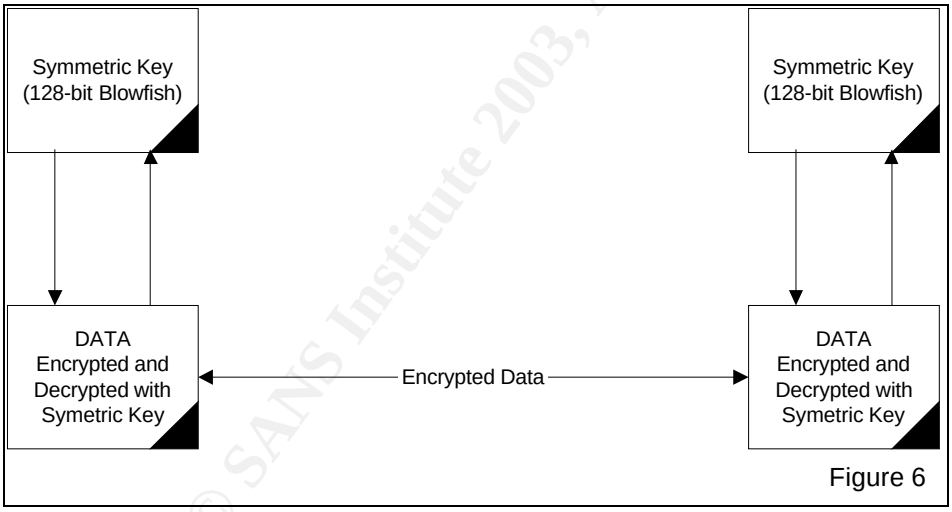


Figure 6

(Palmgren, 2003).

The Diffie-Hellman key exchange primary limitation is in a susceptibility to man-in-the-middle attacks. This type of attack occurs in the following manner:

- User A sends his public key to User B, User C intercepts the key and sends his public key to User B instead.
- Upon receiving the key, User B sends his public key back to User A. User C intercepts the key and sends his key to User A.
- User A and User C agree on one shared key, while User B and User C agree on another shared key.
- After this, User C decrypts any message sent out by User A or User B, reads and modifies them, re-encrypts them with appropriate shared key and sends them to the perspective user.

("3.6.1 What", 2003)

This traditional limitation can be resolved by incorporating digital certificates and the station-to-station protocol. In the case of Trillian, users connect via authentication to the IM vendor specific servers. A specific user is selected to start a Secure IM session and an assumption is made that the individual logged in is that particular user. At this time, the Diffie-Hellman process begins. Under these conditions a man-in-the-middle attack is less likely. It would be more likely for someone to crack a user's password and attempt to impersonate a user, than to try to act as a middle man.

The Diffie-Hellman key exchange process has been in existence for over 25 years. Outside the man-in-the-middle attack, this process has stood the test of time. It is widely used and accepted in the industry as a leader in securely passing keys.

B. Trillian Encryption – 128-bit Blowfish Encryption

Trillian uses 128-bit Blowfish symmetrical keys for data transmission. Symmetrical keys are used instead of asymmetrical keys, because they provide faster data transmission. Also, encryption and decryption of data takes place more effectively than in a system with asymmetrical keys.

Blowfish is a block cipher designed in 1993 by Bruce Schneier as a fast and free alternative to existing encryption algorithms. Blowfish has been analyzed for the past 10 years and no significant weakness has been found in the algorithm. Because of its strength it has been implemented in over 130 commercial applications. Blowfish uses a 64-bit block cipher which means it encrypts and decrypts data in chunks of 64-bits. The key length varies from 32 to 448 bits. Trillian uses a 128-bit key length ("Blowfish Encryption", 2003).

A block cipher such as Blowfish can be explained in simple terms through Figure 7. The block cipher uses a mathematical computation in order to transform the Plaintext Block and the Key into a Ciphertext Block output ("Block Cipher", 2003). The mathematical process is significantly complex in nature. In general, the algorithm consists of a data-encryption piece that converts the 128-bit key into several sub key arrays. Data-encryption occurs via 16 passes through the complex set of key and data-dependent substitutions and permutations (Schneier, 2003).

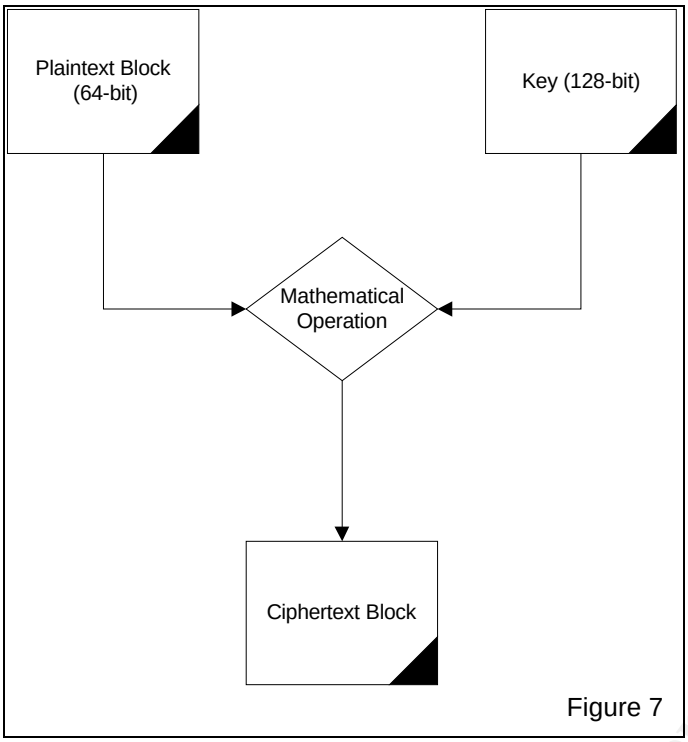


Figure 7

Although effective in encrypting and decrypting the data, a larger key would prove more valuable and secure. The larger the key, the more difficult it would be to crack, so it is recommended that Trillian move to a larger key at some point.

V. Analysis of Ethereal Traffic

An analysis of the underlining packets between AOL IM communications using the AOL client application and Trillian provides the highest level of evidence that normal IM traffic is not secure. In comparison, Trillian client to Trillian client Secure IM obscures the traffic through data encryption. The following paragraphs detail the findings from a practical exercise setup to monitor the network packets. Three scenarios were tested and monitored. All scenarios used AOL as the IM provider. The specific client applications connecting to AOL servers were the AOL client version 5.1.3036 and the Trillian client application version .74. The first scenario used AOL client to AOL client communication, or normal AOL user traffic. The second scenario consisted of one Trillian client user and one AOL client user. The third scenario consisted of two Trillian client users connecting to AOL IM servers. The monitoring tool used for the analysis was Ethereal. Ethereal is a freely distributed monitoring application. It can be used on Unix and Windows platforms to examine data from a live network or from a capture file stored on disk ("Ethereal Home", 2003). Ethereal was run from one of the two client machines to monitor all inbound and outbound network communications. The interface used was the network adapter of the source user. The same accounts were used in each scenario. The full set of scenario screen prints is available in Appendix B. This section contains a subset of the screen prints showing the most relevant data

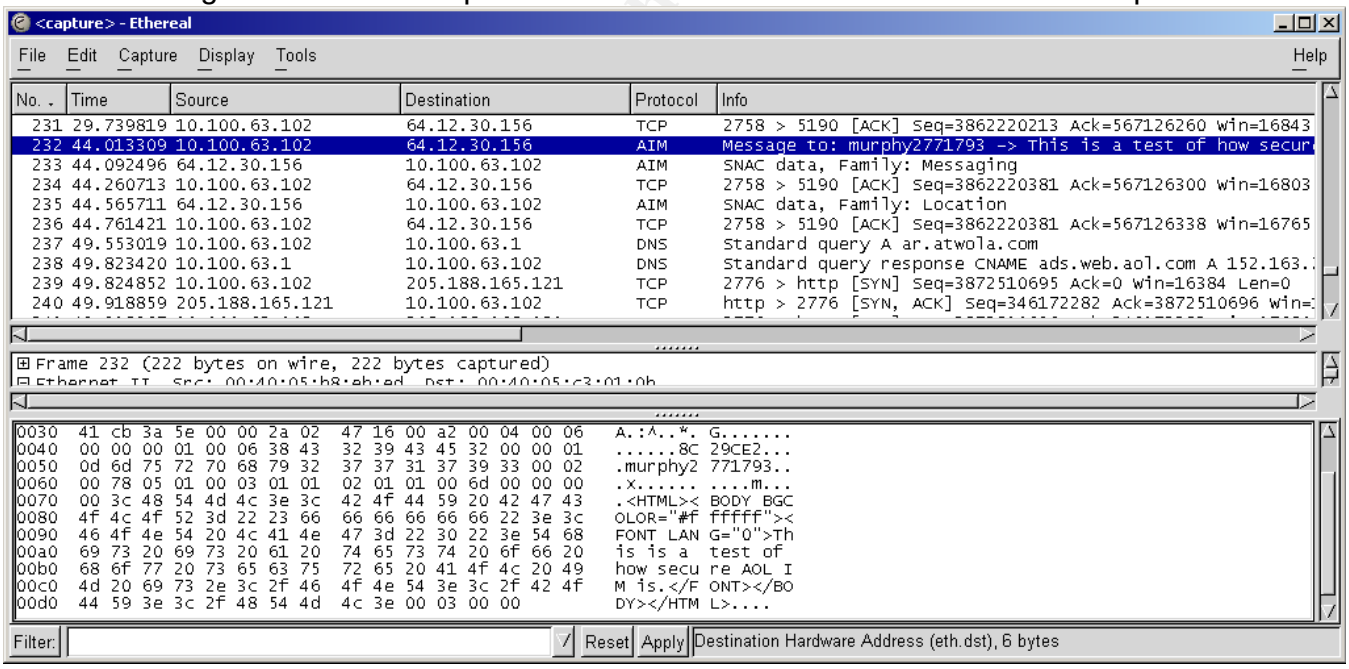
supporting this paper's conclusion that Trillian client to Trillian client network communications are secure between two AOL users.

A. Analysis of Standard AOL IM Network Packets

In scenario one, the traffic of two AOL client users using AOL Instant Messenger version 5.1.3036 was examined. In the screenshot below, line 233 of the Ethereal output displays a text message sent to an AOL service user. The content of the message can be clearly seen in the translated hexadecimal packet. The text in the packet that was submitted via plain text across the Internet was:

<HTML><BODY BGCOLOR="#ffffff"><FONT LANG="0">This is a test of how secure AOL IM is.</FONT></BODY></HTML>

It is evident that monitoring of packets for organizations using the AOL Instant Messenger will reveal that communications are not being submitted securely. Users must understand that even when both are on the same corporate network, IM traffic is transmitted from one user to another via the Internet. The potential for compromising corporate data is very high. The only method to stop leaking confidential information is through training and policies. These policies will deter but not prevent employees from communicating data across an open network that should not be available to the public.



B. Analysis of Trillian to AOL IM network packets

The second scenario examines the usage of Cerulean Studios' Trillian v .74 and AOL Instant Messenger. The communications in this example were not secured, because Trillian was not able to establish and transfer the key encryption key using Diffie-Hellman. Because of this, data flows insecurely between users. This is a potential

problem with users of Trillian. It should be made clear that Trillian users are only securely submitting Instant Messages when communicating with another Trillian user, using AOL or ICQ type messages. Trillian users will see feedback when a secure session has been established.

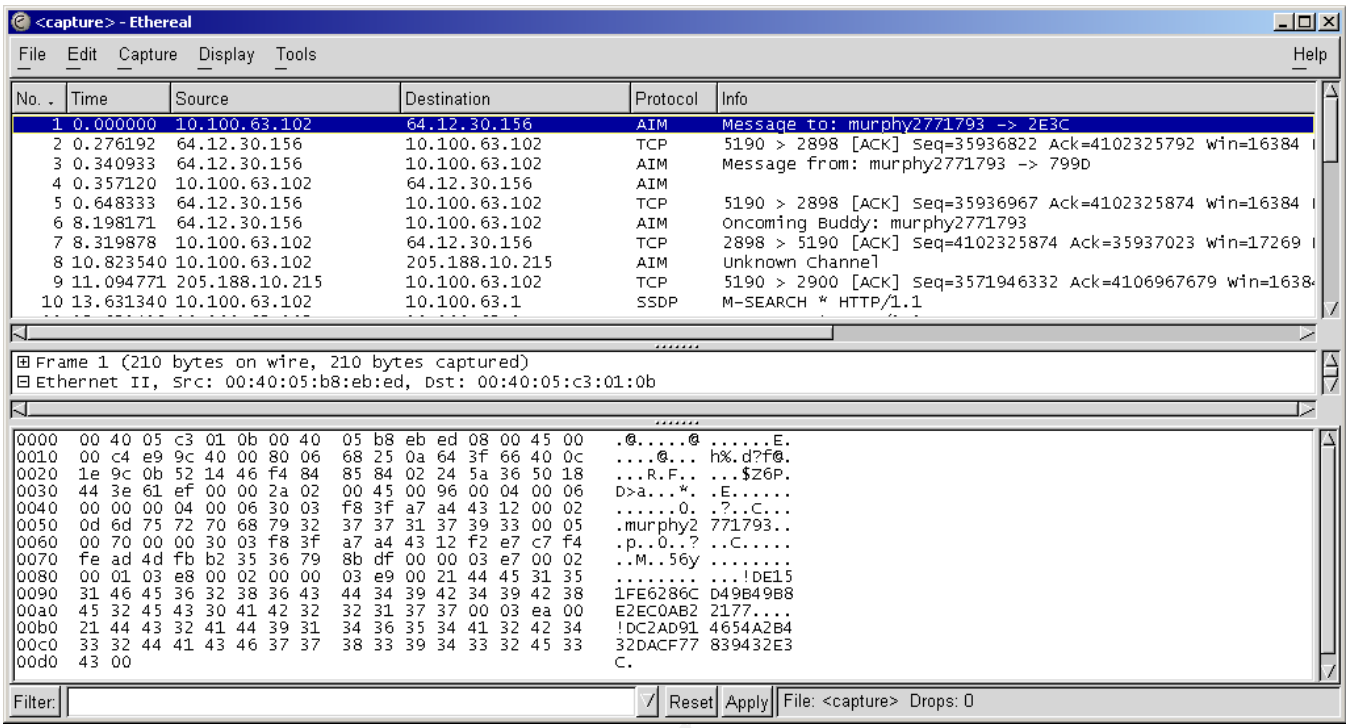
C. Analysis of Trillian Encryption IM Network Packets

The third scenario examines communications between two Cerulean Studios' Trillian users. Both users have selected in their preferences to activate Secure IM. In addition, both users have selected to maintain a Secure IM connection with contacts. These settings are found under Properties, Chatting Services, AIM, Misc. Both "Activate SecureIM Capabilities" and "When possible, make a best effort to automatically maintain a SecureIM session with my contacts" should be checked to enable encryption of AOL and ICQ type transmissions.

The communications initiated between the users when both used Cerulean Studios' Trillian applications resulted in a secure session using the Diffie-Hellman key exchange and 128-bit Blowfish key. During the connection, a user receives visual feedback that a Secure IM session has been started. Below is the example from the scenario test.

Once the connection is established all traffic is securely transferred. In an analysis of the packets it is clear that a communication was sent to the user murphy2771793, but the content of the message has been encrypted and cannot be interpreted. The same HTML message that was displayed in clear text with the AOL application is now transmitted as encrypted data between the two Trillian users:

!DE151FE6286CD49B49B8E2EC0AB22177 ê
!DC2AD914654A2B432DACF77839432E3C



It is evident from this analysis that Trillian adds a layer of security to IM for AOL users that will be beneficial to any organization. Using the packet analysis alone, there is cause for widespread usage of Trillian over the vendor provided AOL client software.

VI. Research Findings

From the research on this product and the analysis of the underlining packets, the following capabilities and limitations are clear.

A. Trillian Capabilities

Trillian has the capability to secure IM communications across the public Internet. The key factors that must be in place to support this capability are:

- The source and target user must both be using Trillian.
- Each Trillian user must use an AOL account. Trillian cannot securely transmit MSN and Yahoo messages.
- Each user must have the appropriate secure communications set in their Trillain preferences.

B. Trillian Limitations

There are some limitations with Trillian that detract from its usefulness. These limitations are listed below:

- Trillian only has the capability to encrypt data for ICQ and AOL. The application does not have the capability to secure MSN or Yahoo IM.
- If one of the two users in communicating does not use Trillian the entire communication with that user will remain insecure.
- Trillian was not designed to be a robust enterprise solution, but it does provide for secure IM with AOL users.
- The main three vendors, Microsoft, AOL Time Warner, and Yahoo, are all pushing for a corporate solution, which may handle filtering in and out public level messages. Trillian will have a difficult time competing with this type of solution if they are successful.
- One final limitation is the key length. Currently the key length is 128-bits, but could potentially be increased to 448-bits. Increasing the size of the key length will result in better overall security.

VII. Conclusion

Widespread usage of Instant Messaging technology has occurred and continues to grow and expand throughout the corporate sector. Using Instant Messaging as a collaboration tool and productivity enhancer must be weighed against the potential security issues associated with IM. From the analysis of Trillian it is clear that the application has positive benefits in the corporate sector. Trillian successfully encrypts data transmission between two Trillian client applications for AOL based IM. Trillian can be used across the Internet with confidence that corporate data is secure. Cerulean Studios has set the bar for corporate level IM with Trillian. Any corporate solution must integrate secure messaging to users outside the corporate Intranet in order for it to viably compete with Trillian. The fact that this solution can be implemented at no cost to individual users is outstanding. Security awareness training is important and should continue to be used in all organizations tailored to the specific IM applications used in the organization. Although Trillian is not flawless, it has great potential and is recommended for all users of the AOL service.

VIII. References

"3.6.1 What is Diffie-Hellman?" RSA Security. http://www.rsasecurity.com/rsalabs/faq/3-6-1.html. April 25, 2003.

"Block Cipher." Wikipedia. http://www.wikipedia.org/wiki/Block_cipher. May 1, 2003.

"Blowfish Encryption." Tropical Software. http://www.tropsoft.com/strongenc/blowfish.htm. April 15, 2003.

"Cerulean Studios' Home Page." Cerulean Studios. http://www.trillian.cc/about/index.html. April 4, 2003.

"Cerulean Studios' Trillian Pro version 1.0 Home Page." Cerulean Studios. http://www.trillian.cc/trillianpro/index.html. April 4, 2003.

"Cerulean Studios' Trillian version .74 Home Page." Cerulean Studios. http://www.trillian.cc/trillian/features-1.html. April 4, 2003.

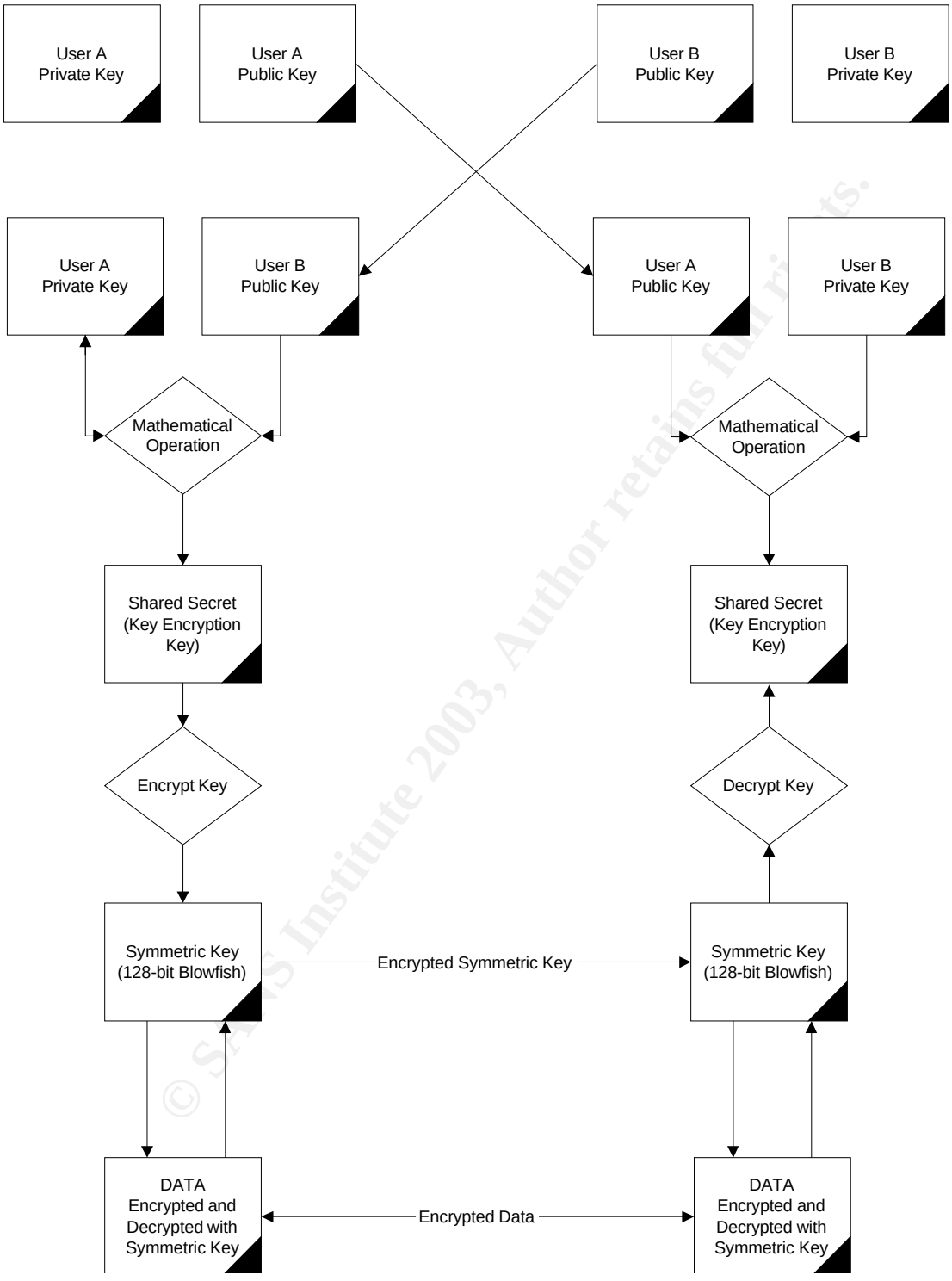
"Collaborative Technologies Critical to the Financial Industry's Development over the Next Three Years." (April 22, 2002). Reuters. http://about.reuters.com/newsreleases/art_22-4-2002_id958.asp. May 17, 2003.

"Ethereal Home Page." Ethereal. http://www.ethereal.com/. May 25, 2003.

Palmgren, Keith. "Diffie-Hellman Key Exchange – A Non-Mathematician's Explanation." NetIP, Inc. http://www.netip.com/articles/keith/diffie-helman.htm. April 17, 2003.

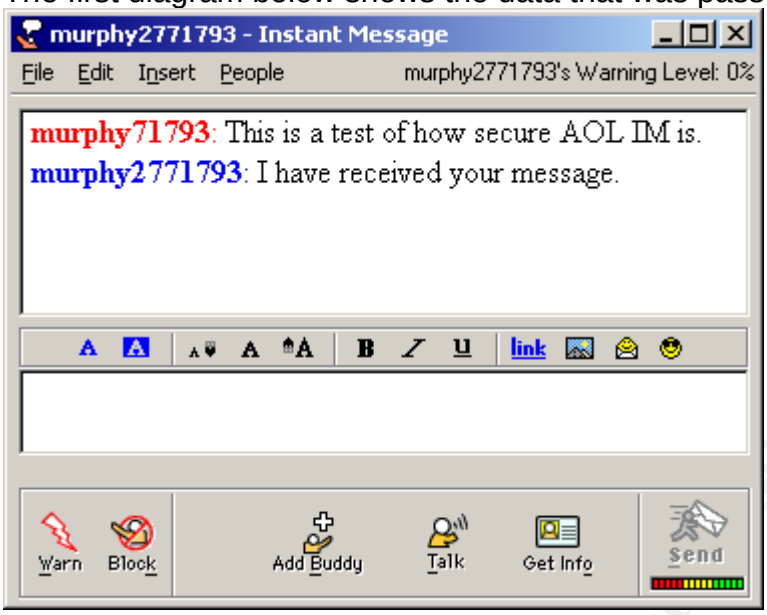
Schneier, B. "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)." Counterpane Internet Security, Inc. http://www.counterpane.com/bfsverlag.html. May 15, 2003.

Appendix A: Trillian Encryption - A combination of Diffie-Hellman Key Exchange and 128-bit Blowfish Symmetric Key

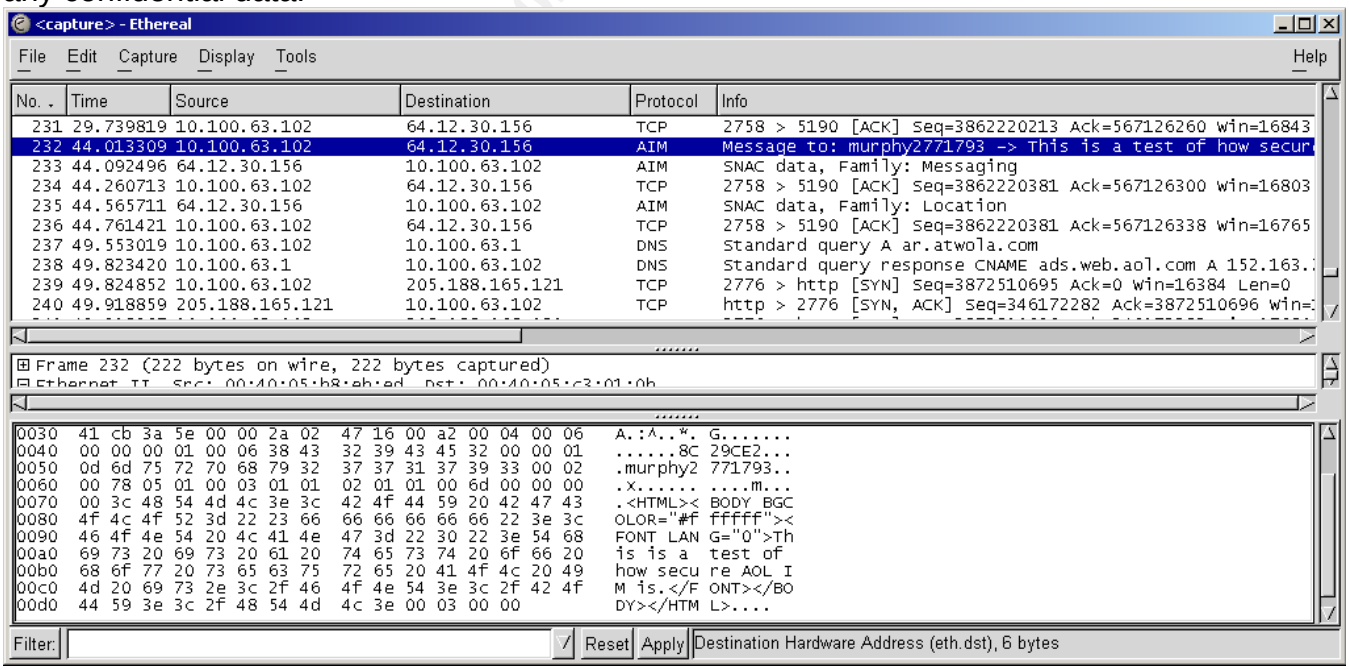


Appendix B: Screen prints and Results of Scenario Testing

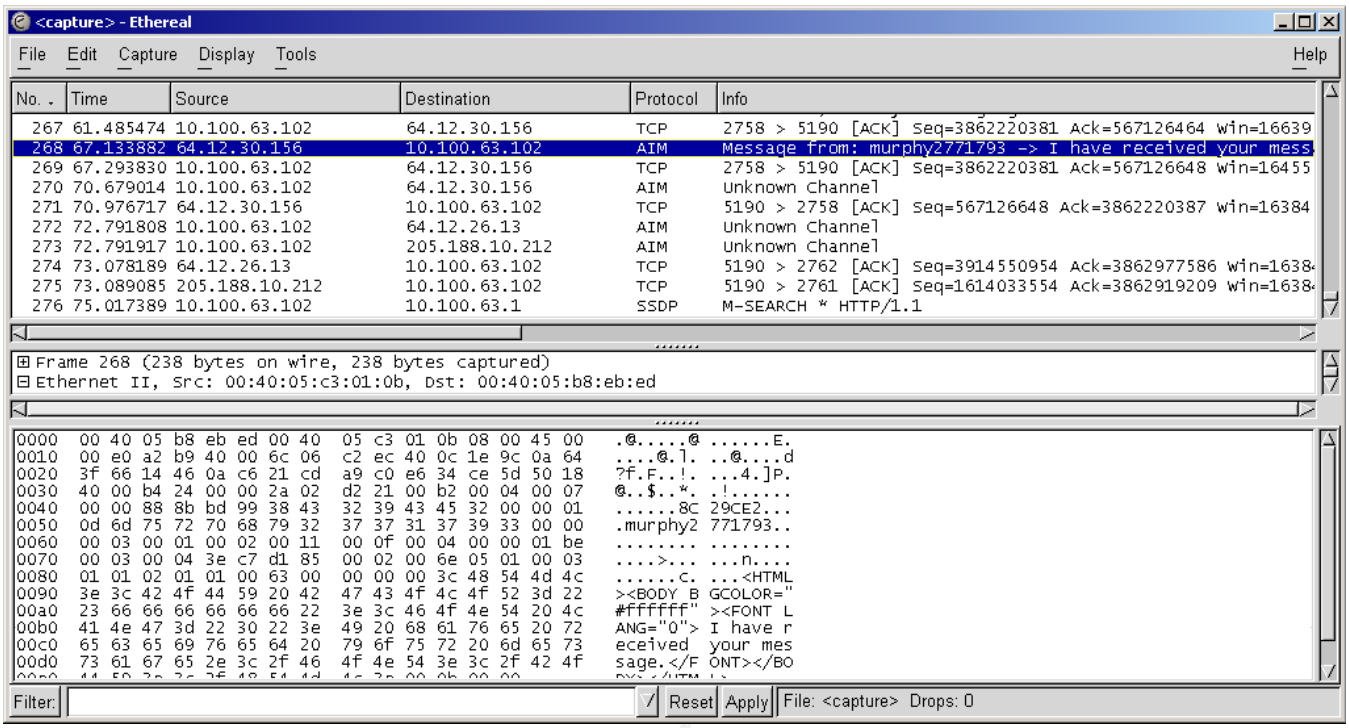
Scenario 1: Communications via two AOL Instant Messenger clients version 5.1.3036. The first diagram below shows the data that was passed between the two users.

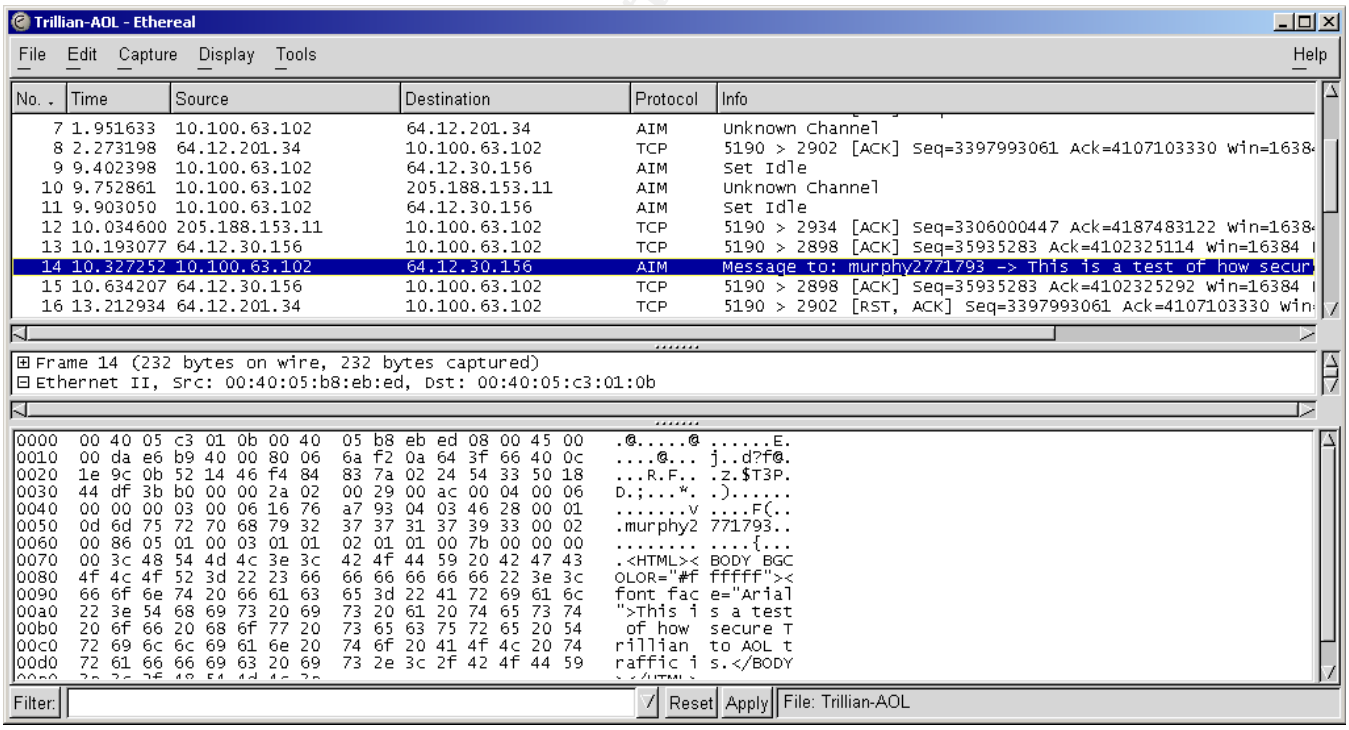


The following Ethereal packet breakdown shows the message sent from murphy71793 to murphy2771793. The data is submitted via plain text between the two users. The data flows across the Internet where hackers could analyze the packets and easily pull any confidential data.

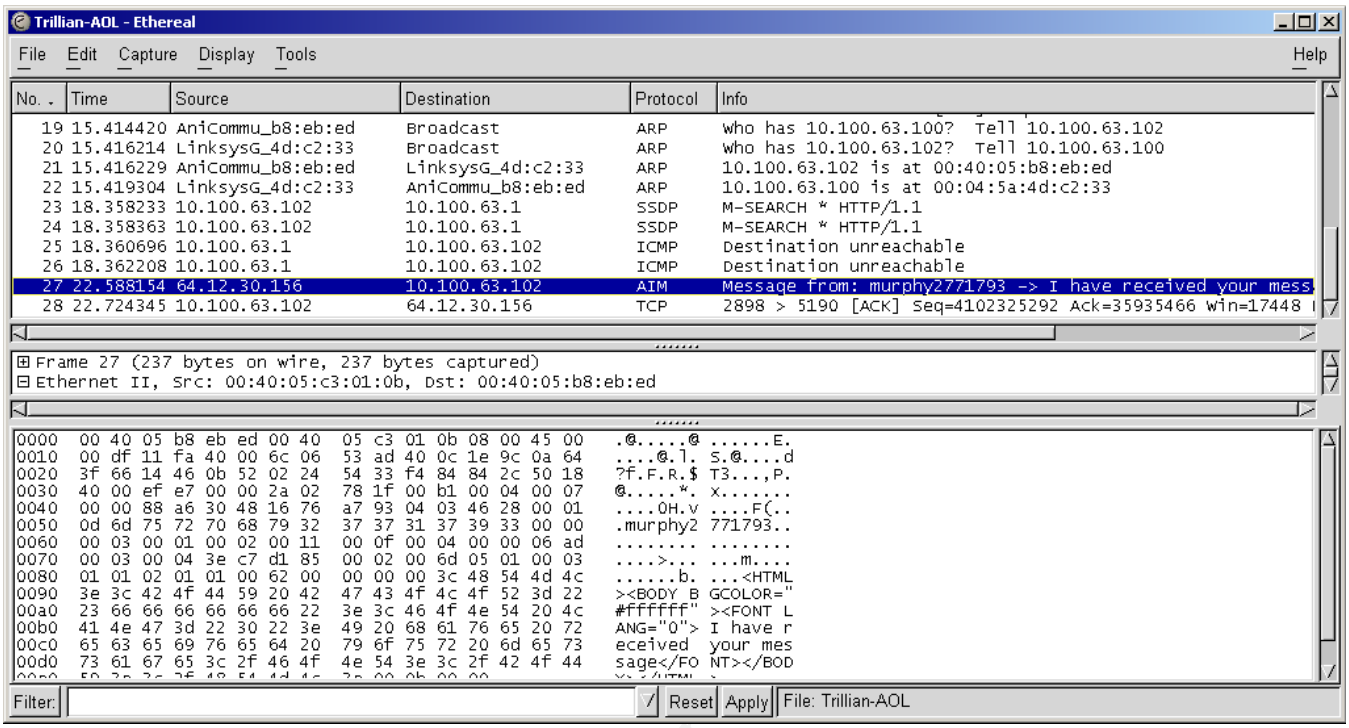


The next screenshot is of the response from murphy2771793 to murphy71793. Again the communication is passed in plain text.

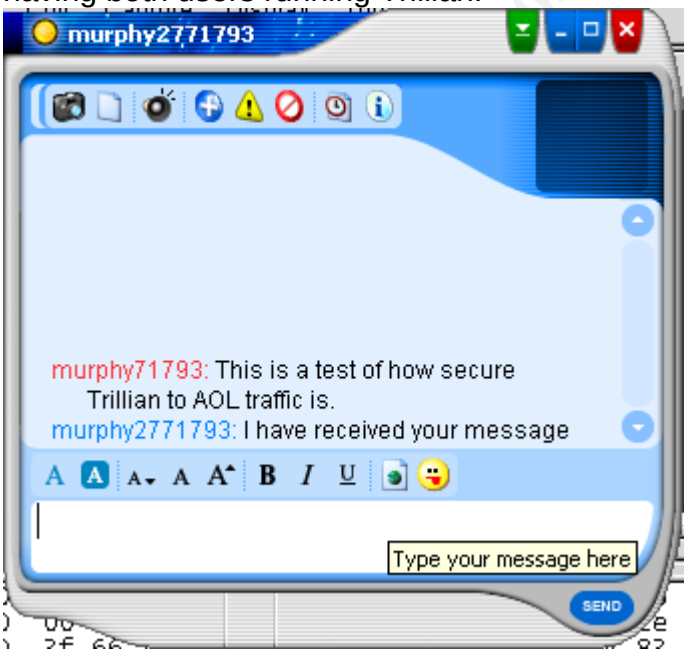




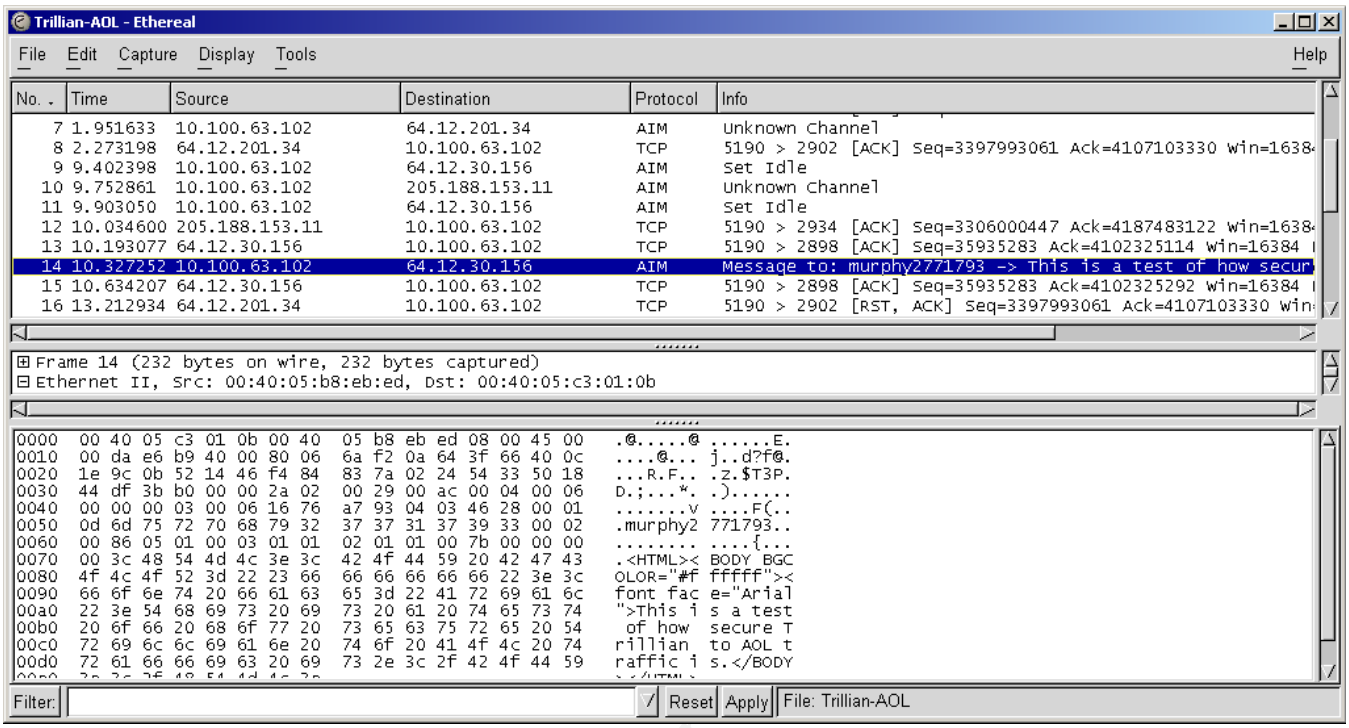
The response, as expected, is also unsecure.



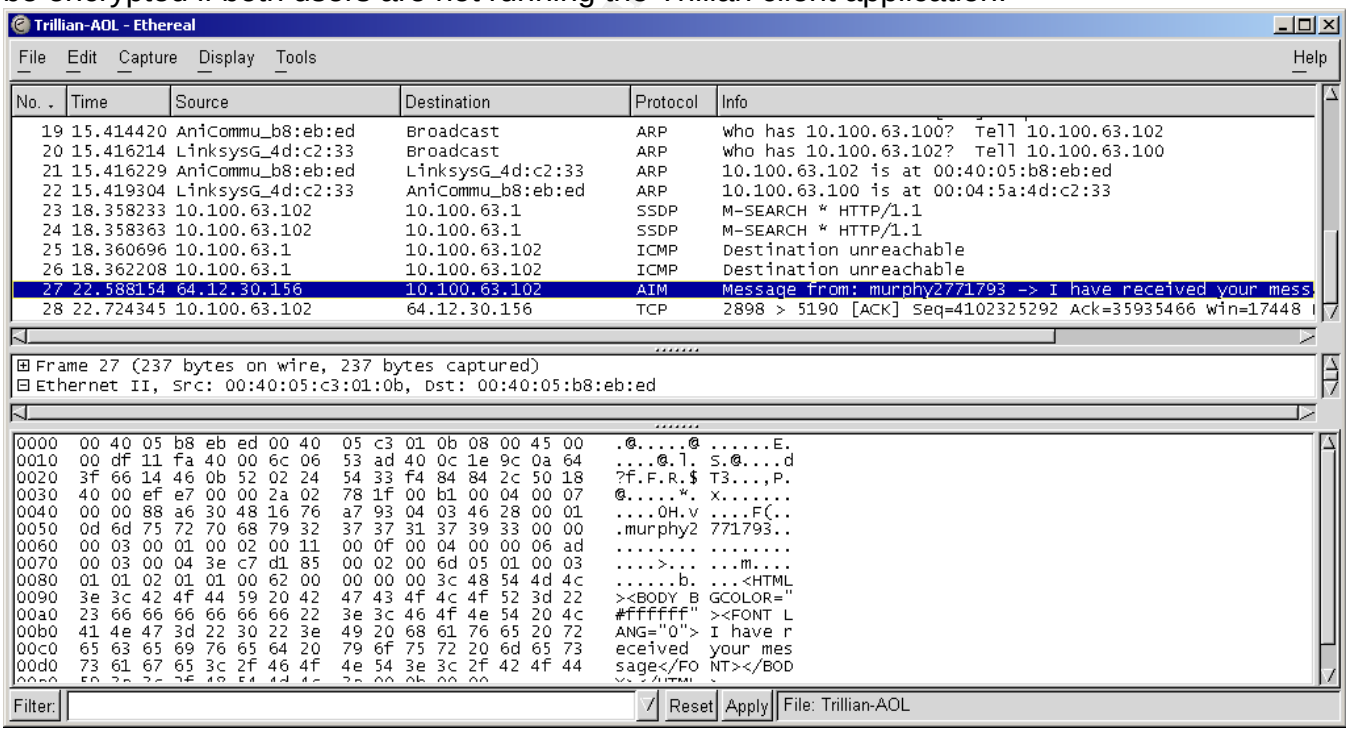
Scenario 2: This scenario examines AOL communications via one AOL client application and one Cerulean Studios' Trillian client application. The first screen print shows the data passed between the two users. Notice that even though Trillian is used, no feedback is given as far as establishing a Secure IM session. This is a result of not having both users running Trillian.



Similar to the Scenario 1, Ethereal reveals the AOL IM packets transferring across the network and they are clearly not encrypted, even though one user has Trillian.



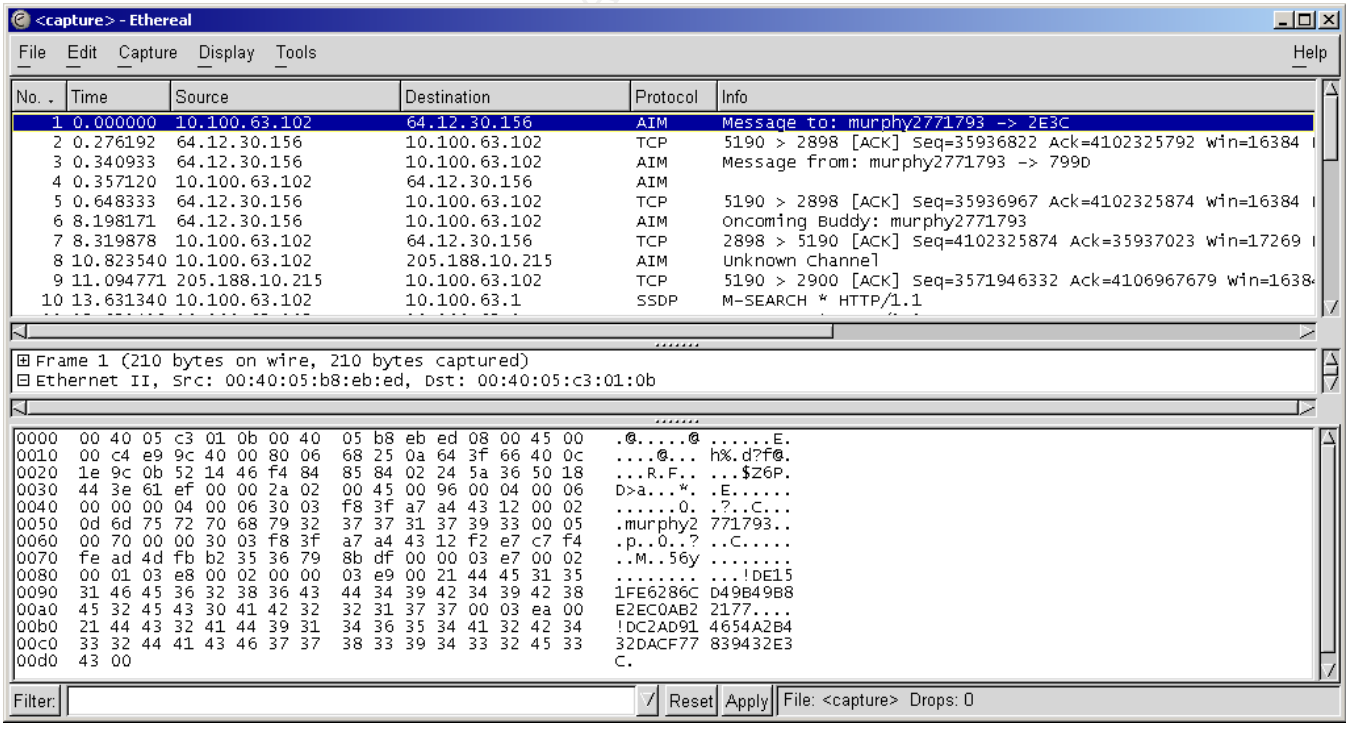
The response message is also sent in clear text without encryption. The data can not be encrypted if both users are not running the Trillian client application.



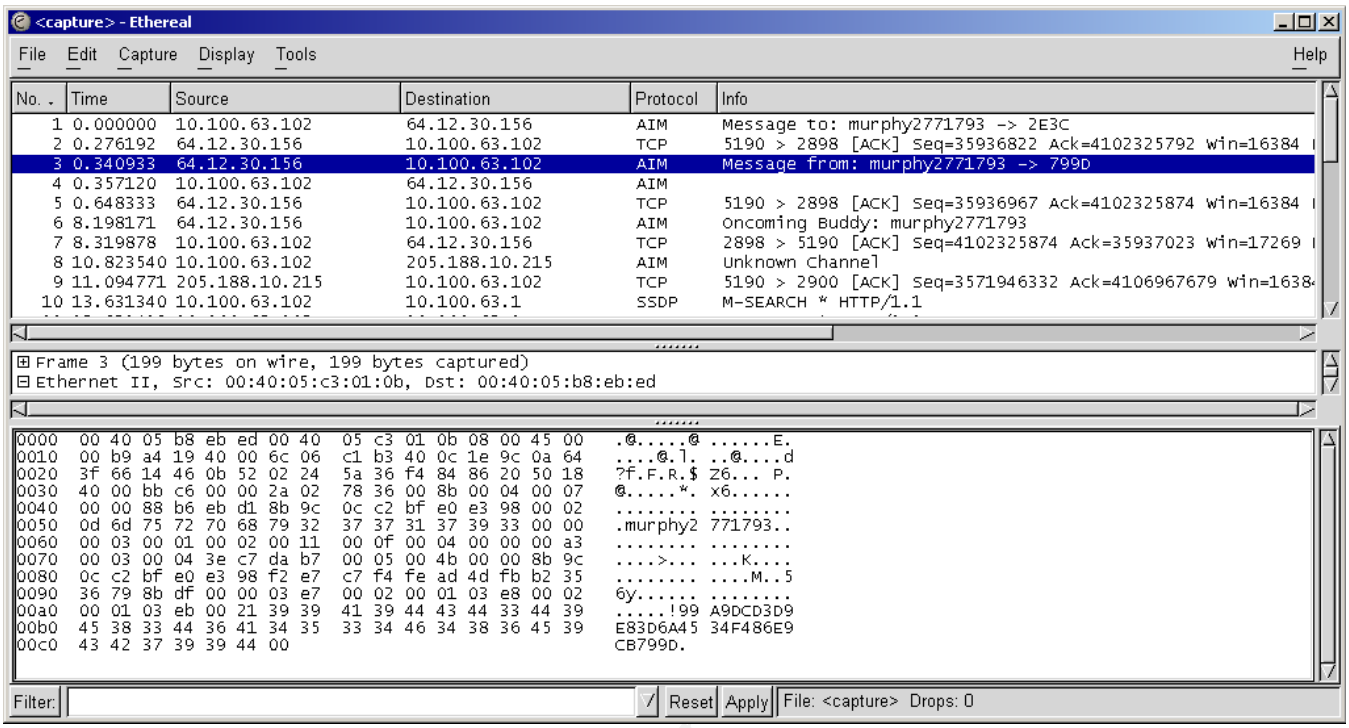
Scenario 3: This scenario examines AOL communications via two Cerulean Studios' Trillian users. The first screen print shows murphy71793 establishing a Secure IM

session with Murphy2771793. This feedback is always present when creating Secure IM sessions.

In this case Ethereal does reveal that there are AOL IM (AIM) packets transferring across the network, but as seen in the raw data, Ethereal cannot interpret the encrypted data.



The response message is also encrypted. This case displays that when using Trillian client on both ends of an IM communication, that all data transmits as encrypted data.



Trillian successfully establishes and maintains a Secure IM session between the two users in the third scenario.