Unsecured sessions with ICQ
- applying forensic computing

Martin Kling
This thesis is submitted to the Department of Software Engineering and Computer Science at Blekinge Institute of Technology in partial fulfillment of the requirements for the degree of Master of Science in Computer Science. The thesis is equivalent to 20 weeks of full time studies.

Contact Information:
Author: Martin Kling
Address: Fältv 17
       SE-291 39 Kristianstad
E-mail: martinkling@hotmail.com
Phone: +46733691999

External advisor:
Tony Möörk
Swedish National Criminal Investigation Department
Information Technology Crime Squad
P.O Box 12256
SE-102 26 Stockholm
Sweden
Phone: +46 8 401 48 41

University advisor:
Ph.D. Bengt Carlsson
Department of Software Engineering and Computer Science

Department of
Software Engineering and Computer Science
Blekinge Institute of Technology
Box 520
SE – 372 25 Ronneby
Sweden

Internet: www.bth.se/ipd
Phone: +46 457 38 50 00
Fax: + 46 457 271 25
Abstract

Digital evidence is becoming more and more frequent and important in investigations carried out by the police. To make the correct judgements, the police force needs to know what one can do with ICQ and in what ways it can be exploited.

This thesis aims to point out weaknesses in ICQ that can aid the police in their work. But these weaknesses can not only be used by the police, also crackers can perform malicious acts with them. Therefore, I investigated if the use of ICQ resulted in non-secure sessions.

To investigate ICQ’s security, I divided a session into an authentication phase, sending of messages, and the protection of stored messages in a history file. While investigating ICQ, I sniffered its Internet traffic and monitored files on the computer’s hard drive with MD5 checksums. I have investigated the following three ICQ applications: ICQ Pro 2003a, ICQ2Go and the Linux clone Licq.

The result of the entire investigation showed that ICQ had a non-secured authentication phase, non-secured messages and no protection for stored messages. From these results the main conclusion was derived: The use of ICQ resulted in non-secure instant messaging sessions.

Your ICQ account can be hijacked and another person can impersonate you and send messages that you dislike. Also, your messages can be intercepted on the Internet and their content can be read. If your computer is compromised, all your previous messages on ICQ Pro 2003a and Licq can be read.

Keywords: ICQ, Instant Messaging, Forensic computing, Digital evidence.
Acknowledgements

I send my thanks to the following persons:

Bengt Carlsson, my supervisor, for the guidance and help in the production of this thesis.

Tobias Bondesson, my cousin, for insightful feedback, on content and language.

Also thanks to those at the Department of Software Engineering and Computer Science, at the Blekinge Institute of Technology, who has made my investigations at the security lab possible and assisted with their guidance.
Contents

1 Introduction .........................................................................................................................................................1
  1.1 Delimitations .................................................................................................................................................. 2
  1.2 Hypothesis ...................................................................................................................................................... 3
    1.2.1 Authentication process .......................................................................................................................... 3
    1.2.2 Messages .................................................................................................................................................. 3
    1.2.3 ICQ History .............................................................................................................................................. 4
2 Instant messaging ............................................................................................................................................... 5
  2.1 Predecessors of Instant Messaging ............................................................................................................. 5
  2.2 ICQ ................................................................................................................................................................. 6
    2.2.1 The ICQ protocol ...................................................................................................................................... 7
3 Security .............................................................................................................................................................. 8
  3.1 Forensic computing ....................................................................................................................................... 8
  3.2 Sniffing ........................................................................................................................................................... 8
  3.3 Encryption ..................................................................................................................................................... 9
  3.4 MD5 checksums .......................................................................................................................................... 10
  3.5 ICQ Security ................................................................................................................................................ 11
4 Investigation ...................................................................................................................................................... 13
  4.1 Investigating ICQ .......................................................................................................................................... 13
    4.1.1 tcpdump and WinDump .......................................................................................................................... 14
    4.1.2 Ethereal .................................................................................................................................................. 14
    4.1.3 MD5 ....................................................................................................................................................... 14
    4.1.4 ICQ database to XML converter ............................................................................................................ 15
  4.2 Workflow ...................................................................................................................................................... 15
    4.2.1 Authentication phase ............................................................................................................................ 15
    4.2.2 Messages .............................................................................................................................................. 16
    4.2.3 ICQ history .............................................................................................................................................. 17
5 Result ............................................................................................................................................................... 18
  5.1 Authentication phase .................................................................................................................................... 18
    5.1.1 Analyzing the authentication phase ...................................................................................................... 18
  5.2 Messages ...................................................................................................................................................... 19
    5.2.1 Analyzing the messages phase ............................................................................................................... 20
  5.3 ICQ History .................................................................................................................................................. 21
    5.3.1 Analyzing the ICQ history ...................................................................................................................... 21
  5.4 Results .......................................................................................................................................................... 22
6 Discussion .......................................................................................................................................................... 23
  6.1 Validity and reliability of the investigation ................................................................................................. 23
  6.2 ICQ security .................................................................................................................................................. 23
    6.2.1 SSL and encryption? ............................................................................................................................ 24
6.2.2 AOL and ICQ ...................................................... 24
6.2.3 ICQ in the future ................................................. 24
6.3 Future studies ...................................................... 25

7 Conclusion .......................................................... 26
8 References .......................................................... 27

Appendix 1 .................................................................. 29
Appendix 2 .................................................................. 30
Appendix 3 .................................................................. 31
1 Introduction

The following is a description of a scenario, which can occur when using ICQ. The scenario contains three persons:

- Max, an honest university student
- Sue, a not so honest university student (cracker)
- Carl, Chief Executive Officer of a smaller company.

Carl has sent out e-mails to a University in hope of employing a person who is about to graduate this summer. After replying to Carl’s e-mail to report her interest in the job, Sue receives Carl’s ICQ number (UIN) so they can communicate and discuss the employment via ICQ. Sue is not only a technically skilled student—she also likes to sniff the student network. Since Sue is very interested in working for Carl she listens if there is any ICQ traffic on the student network between another student and Carl.

One day, Sue spots traffic between her classmate Max and Carl. Since Max is a very bright and clever person, Sue decides she must discredit Max or risk losing the job. She has read on the Internet that ICQ accounts are easy to crack and decides to try to break Max’s password.

The next time Max logs into his ICQ account, Sue’s sniffer application records the transmissions. She then extracts the encrypted password and decrypts it by using the key she found on the Internet.

Now Sue has everything she needs to complete her plan. The next time Max shuts down his ICQ and goes to class, Sue is ready to start. Since Sue does not want to leave any traces, she starts the web based service ICQ2Go. Sue then enters Max’s UIN and password and is logged into his account. When connected, she automatically receives Max’s contact list via Internet.

Sue sends a message to the CEO Carl to establish contact. Carl is completely fooled by Sue and thinks he is talking to Max. Sue tells Carl she (“Max”) is not interested in the job anymore. Carl then removes Max from the list of possible employees. Sue has through her skills removed Max from the competition for the vacancy.

This example is made up and may never have happened. However, the technique is available, so similar actions may have occurred. Chat tools can be fooled with today’s technology, but there are also other aspects to them. They create a privacy that makes them popular to criminal activity. Because of this, digital evidence is becoming more and more frequent and important in police investigations. Information extracted from ICQ can help either to dismiss or point out a suspect. To make the correct judgements, the police force has to know what can be done with ICQ and in what ways it can be exploited.
To investigate how ICQ works is therefore of interest from a juridical point of view. Also, the subject of ICQ-security is of interest to the scientific community as well as to ICQ users.

This thesis targets the following groups:

- people working with collecting digital evidence
- people interested in having secure communication with instant messaging (IM) and ICQ (pronounced I Seek You)
- people interested in Information Security

This thesis aims to point out weaknesses in ICQ that can aid the police in their work. However, the police are not the only group that can use these weaknesses. On the Internet, instructions can be found describing how to perform malicious acts on ICQ. What can be an asset to the police can therefore be a security risk for the user.

In an article, André Rickardsson claims IM-clients to be security holes and that 80% of the business users of IM say that they have not heard of any restrictions in the use of IM software on their workplace. [Nordner, 2003] Osterman Research made an investigation in May 2002 and found that in 84% of the surveyed companies people were using IM software. [Osterman, 2002]

I will in this thesis mention various malicious persons. I will refer to these as crackers. A cracker is a person who performs malicious acts with computers, e.g. password breaking. The cracker is distinguished by his illegal and vicious activities, as opposed to the hacker.

To understand much of the contents of this thesis, the reader must have a basic familiarity with TCP/IP and how packets are sent over networks and the Internet.

## 1.1 Delimitations

This thesis is delimited to the three ICQ applications ICQ Pro 2003a, ICQ2Go and Licq. These applications, among the most used ICQ applications, will be studied with their default settings. ICQ Pro 2003a and ICQ2Go will be tested on Microsoft Windows XP. The Linux clone Licq will be tested on the operating system Red Hat 8.0. I will in this thesis not try to recover deleted files or extract data from page files or from RAM. The thesis is further restricted to the questions mentioned in section 1.2.
1.2 Hypothesis

There are sources claiming ICQ to be an insecure application e.g. ISS [2000] and Hansen [2000]. I have therefore tested ICQ and then analyzed the results to see if it resulted in non-secure communication.

My hypothesis reads as follows:

**The use of the instant messaging application ICQ results in non-secure sessions.**

To help draw conclusions from the hypothesis I will answer the following questions:

- In what way does ICQ secure your authentication process?
- In what way does ICQ secure your messages from wiretapping?
- In what way does ICQ secure your history file from forensic computing?

The authentication process, communication and the storing of messages are collectively referred to as a session in this thesis.

1.2.1 Authentication process

According to Massimo Melina, the unique ICQ number, later referred to as the UIN, and the encrypted password are transported in the same TCP packet. In addition, the encryption on the password is weak and easy to crack. [Melina, 2002] I will test if this is true since weak protection is a serious security concern, e.g. enabling the theft and impersonation of other persons’ identities. [ISS, 2000] If your account has been hijacked, the perpetrator can commit criminal actions in your name.

I will investigate if the authentication process is secured and if the authentication packet is easy to locate in a dump file over network traffic.

1.2.2 Messages

Internet Security Systems claims in a report from 2000 that ICQ messages are sent unencrypted. They also conclude that all information sent over ICQ must be regarded as public, due to the lack of encryption. [ISS, 2000] This means that you should not send anything over ICQ that you want to keep secret.

I will use the forensic technique to record digital evidence at the data-link layer and investigate if messages are being sent encrypted or unencrypted. I will also see if ICQ
traffic uses standardized ports for easy recognition and if the traffic passes through an ICQ-server.

1.2.3 ICQ History
ICQ logs all sent messages in a file saved on the local user’s computer. If you gain access to this computer, you can see all ICQ communication made from there. This is a great feature for those who want to see what they have written before, but it is also a security threat if secrets are revealed. [ISS, 2000]

I will use a forensic technique to try to extract digital evidence from a computer file and investigate if the ICQ history file is encrypted or unencrypted. ICQ2Go does not use any history file so I will see if it leaves any other evidence on the used computer.
2 INSTANT MESSAGING

Before presenting ICQ, I will look at predecessors to instant messaging. First, however, I will explain what instant messaging (IM) is.

Instant messaging is the exchange of messages over the Internet. Both the sender and the receiver should be connected to the Internet at the time of the transmission. The difference between e-mail and IM is that IM messages are relayed directly to the receiver without storing them on a server.

![Diagram of instant messaging sequence](image)

Figure 2.1, The instant messaging sequence [Lotson, 2003a]

2.1 Predecessors of Instant Messaging

The development towards the first instant messaging application came when Jeff Kell started to exchange messages with a colleague. They worked over an IBM 360 mainframe without monitors. Kell became inspired and started to write a chat program. The application was clumsy to use and consumed a lot of bandwidth in Bitnet which was a university network in Europe and the US. [Lotsson, 2003b]

In 1985, Jeff Kell released a chat application named Relay. The way Relay worked on Bitnet became a role model for the development of Internet Relay Chat (IRC), which was released in 1988. [Lotsson, 2003b] IRC can be used by anyone with Internet access and the software is free or low-cost. [Casey, 2000] mIRC is the most used IRC client and offers you the possibility to connect to chat rooms all over the world. The IRC network is made up from different servers maintained by different groups of people. These servers are referred to as subnets, e.g. Undernet, DALnet and IRCnet. [Casey, 2000]

IRC allows people chatting on a chat group to generate a direct connection between their computers. This allows information to be sent, without passing through an IRC server, as a peer-to-peer transmission. Meanwhile, IRC servers do not record events
made by users. This makes IRC popular to groups discussing illegal activities. Since it is even possible to transfer files between users, child pornographers, among others, are very fond of IRC. [Casey, 2000]

Besides Kell’s applications, direct messaging has always been found in systems using Unix. Unix systems allowed messages to be sent from a user to another on the same network. If the user was not logged in on his computer the message was stored for later reading. [Lotsson, 2003a]

IRC and Unix massaging were born before the nineties. After that, the Internet boom came with new technologies and ideas; it was time for ICQ to emerge.

### 2.2 ICQ

ICQ (pronounced I Seek You) was the first widespread application for instant messaging. The Israeli company Mirabilis released its first version in 1996 and ICQ grew rapidly. In June 1997 there were 100,000 people logged in simultaneous on the IM service. In June 1998 Mirabilis was bought by America Online for USD 287 million and changed its name to ICQ Inc.

Since then, ICQ has then been developed through numerous versions, among others ICQ 98, and the latest ICQ Pro 2003a. ICQ now exist in several applications for which ICQ Inc. has developed three applications ICQ Pro2003a, ICQ Lite, and ICQ2Go. Other applications that can communicate via ICQ are Trillian and Licq.

You log on to the ICQ network using your unique ICQ number, called UIN (Unique Internet Number), and a password. ICQ uses a service called presence service which, when you come online, notifies you of which contacts on your buddy list are online.

![ICQ login sequence](image)

*Figure 2.2, The ICQ login sequence, with the update of buddy list [Lotsson, 2003a]*
ICQ is implemented so that it will not have to consume all your focus. It is like “send and forget”; you send a message and then continue surfing, writing or what you were doing. When you receive a message, you will be notified by a sound and a flashing message in the system tray or taskbar.

A more active way of communicating is to enter chat mode. In chat mode you see every character that your chat friend enters without delaying for a carriage return. The applications in my investigation having the chat feature are Licq and ICQ Pro 2003a.

When downloading ICQ Pro 2003a you acquire a 3.8 MB large installer. When the installer is activated, you are guided through a setup process. After installation, ICQ can either start automatically on Windows start up or manually through a shortcut on the desktop.

ICQ2Go is a Web based ICQ application released by ICQ Inc. You do not have to download an application to use it but you must have Microsoft Virtual Machine installed. ICQ2Go works on any computer that has a browser with Java support. ICQ2Go is started by entering http://go.icq.com.

ICQ Inc. has not released any ported version of ICQ to work on Linux. ICQ applications for Linux system are therefore called clones. Licq is an ICQ clone that comes with many Linux releases, e.g. Red Hat and Mandrake, and is the most downloaded Linux clone on download.com (May, 2003). Licq is released under the GNU General Public License. The idea behind GNU GPL is that software is free and that you can make alterations in the source code.

2.2.1 The ICQ protocol

ICQ2002 uses ICQ protocol version 8 (ICQv8) [Melina, 2002] and ICQ 2003a probably uses ICQv9. ICQv8 is based on OSCAR (Open System for Communication in Realtime), a protocol developed by America Online (AOL). This protocol was developed for AOL’s chat client AIM (AOL Instant Messenger) but is since ICQ2000 used by ICQ applications. [ISS Oscar, 2003] There is no official information about the protocol, but information can be found on the Internet from people that have reverse engineered the ICQ protocol and written down the specifications.

Licq uses a reverse engineered version of the ICQ protocol and fools the ICQ network that it is an ICQ 2001b client. ICQ2Go uses a protocol of its own since it does not communicate directly to any other applications.
3 SECURITY

In this chapter, I will present what sniffing is and how it works. I will also present the securing, symmetric encryption and the authenticating message digest function MD5. Finally, I will deal with ICQ security. First, however, I will present what forensic computing is.

3.1 Forensic computing

Forensic computing [Casey, 2000] applies under forensic science. Forensic science contains techniques used for “identifying, recovering, reconstructing, or analyzing evidence during a criminal investigation.” It uses so-called digital evidence to link a suspect or victim to a crime.

Digital evidence is subject to the same rules as physical evidence and must be admissible. Otherwise, it will be treated as hearsay. However, digital evidence has advantages over physical evidence. Among others, it can be duplicated so you can compare a copy with the original in court to prove authenticity. That it is hard to destroy is another advantage since even deleted files can be extracted from a disk.

Evidence can be found at the application layer, transport/network layer and data-link/physical layer. Web browsers keep records about visited pages at the application layer. On the transport and network layer investigators of a crime can find IP addresses to determine whom the sender and the receiver of a message connected to a crime was.

The data-link/physical layer is a “gold-mine” of evidence. The sender can be identified by the MAC (Media Access Control) address and if an investigator can, and is, allowed to sniff the network, he or she will have unlimited access to all network traffic.

3.2 Sniffing

In the Internet-world, two main types of threats are present: passive and active attacks. Active attacks can be to flood/hack a node on the Internet or to hijack sessions. A passive attack can be to eavesdrop on transmissions over the Internet using a sniffer tool. [Stallings, 2000]

A sniffer program needs to be located on the same network as the traffic to be monitored. This means that you need to have a computer connected to the network that you want to sniff. [FIST, 1998] Sniffing is made by placing a Network Interface
Card in so-called promiscuous mode allowing all traffic on the network pass through for storing to a file. [Casey, 2000]

Sniffing is a threat against confidentiality. The consequences of a confidentiality attack may be either “loss of information” or “loss of privacy”. [Stallings, 2000] A cracker who has gained access to your network can see all unencrypted traffic that pass by the compromised computer. The dangers with this are the ability to capture passwords, the capture of confidential information, and breaching the security of neighboring networks. [Maximum Security, 2001]

A strategic place for a cracker to locate a sniffer is the gateway for the examined network. This allows the sniffer to record all Internet traffic going to and from that network. A sniffer attack is considered to represent an “extremely high level of risk”. The system has already been broken into and the cracker will be able to see confidential information in the form of e-mails, web traffic and even credit card numbers. [Maximum Security, 2001]

Some cases where a sniffer has been found are at California State University at Stanislaus, a United States Army missile research laboratory, and White Sands Missile Range. [Maximum Security, 2001]

### 3.3 Encryption

Because of Internet’s openness, the use of encryption is necessary for securing your privacy. [Danesh, 2002] The most used form of encryption is called symmetric encryption. When using symmetric encryption, three elements are required:

- A plaintext to be encrypted
- A strong encryption algorithm
- A secret key

The output is a cipher text which can be decrypted by using a decryption algorithm and the secret key. The flow of an encrypted transmission is described in Figure 3.1.

![Figure 3.1, Flow when using symmetric encryption](Stallings, 2000)
The most widely used encryption technique is called Data Encryption Standard (DES), which was adopted by The National Institute of Standards and Technology (NIST) as a standard in 1977. DES divides the file to be encrypted in 64-bit strings and uses a 56-bit key. In 1985, Triple DEA was taken as an ANSI standard in financial applications. TDEA uses three keys and executes the DEA algorithm three times. Since DEA uses a key length of 56 bits, the key in TDEA is 168 bits, making it practically unbreakable by using brute-force methods. [Stallings, 2000]

Encrypted material is of course seen in criminal investigations and is not always possible to decrypt. However, even encrypted digital evidence can be used in an investigation since it can prove that communication has taken place between two or more persons at a particular time. This communication can be used to tie the perpetrator to an accomplice or to a crime. [Casey, 2000]

ICQ uses symmetric encryption as in Figure 3.1 for protecting the password. But it does not use any strong technique like DEA or TDEA.

Encryption is used for concealing content. Sometimes, however, you want to make sure that files have not been altered. For that reason, the message digest function MD5 exists.

3.4 MD5 checksums

MD5 takes a file and produces a 128-bit message digest (32 hexadecimal figures). [Stallings, 2000] The digest is like a file’s fingerprint. It changes if modifications have been made to the file. Two identical files will produce the same digest but even the slightest change will cause huge changes on the MD5 sum. [Casey, 2000]

To demonstrate how the MD5 function works I created a text file with the text “BTH student working”. This gave an MD5 checksum of 8f79b8b0bb199e8d9075ae0d10f16bf. Then I altered the text to “BTh student working” and the MD5 sum was changed to fde5b72b6f4a0bf9786d896aaad4c6d.

There was a very small modification made in the file but the checksum was completely different. This function of the MD5 algorithm makes it popular to use by e.g. computer forensics for securing the authenticity of files and disks. [Casey, 2000]

To detect sniffer attacks, administrators can use an application that creates MD5 fingerprints of the system. These fingerprints later allow comparison for checking if the hard drive’s content has been altered. [FIST, 1998]
3.5 ICQ Security

In a news article from February 2000, the Web casting consultant Dale Ficken was interviewed about the theft of his ICQ account. A cracker had changed his password and locked him out from his account. Ficken used his ICQ account to communicate to business contacts and was therefore greatly affected by the loss. The cracker contacted Ficken with the message “You want your UIN back, I want your 100 dollars.” The AOL representative Rich D’Amato says that they do not know how Fricken’s password was compromised. [Hansen, 2000]

In the privacy agreement from ICQ Inc. you must agree that ICQ is an insecure application. It says in clear text that it can be subject of sniffing, password breaking and several other dangers. But this information is hard to find and has not gone through to the public.

“Also please note that the ICQ software, as with most Internet applications, is vulnerable to various security issues and hence should be considered unsecured”

“data and information on the ICQ Services and Information may be subject to privacy and security invading activities including … eavesdropping, electronic trespassing, sniffing, spamming, nuking, hacking, spoofing, "impersonating", breaking passwords, harassment, fraud, forgery and system contamination …”

Figure 3.2 – Extract from The ICQ Privacy Policy

ICQ Inc. is owned by America Online, one of the world largest corporations. ICQ is also one of the largest IM clients on the market today. People therefore use ICQ as if it were a secure application.

ICQ sometimes operates as a Client/Server architecture for which there are some common security problems. Among the most general issues are forging of identity and malicious program code (viruses, Trojan horses, worms). Another problem is traffic analysis, which includes monitoring addresses, the frequency of messages and their length. [SIG Security, 1993]

Since the Internet is not a secure medium, someone with the appropriate knowledge can intercept messages. If ICQ sessions are in clear-text, these messages will be readable if eavesdropped on. The authentication process on ICQ is encrypted with a weak XOR algorithm which is easy to decipher and its authenticity is therefore threatened by sniffers. [ISS Oscar, 2003]

A strategic place for a cracker to place a sniffer is an ICQ-server. This allows the sniffer to record all ICQ traffic going through that server. This would give him not only the ability to read messages but he could also decrypt passwords and then steal
accounts. If messages pass through a server, the cracker would be able to read the messages content.
4 INVESTIGATION

To investigate ICQ, I sniffed network traffic and created MD5 checksums of hard disks. The following points where investigated:

- The protection of the authentication phase
- The protection of messages
- The protection of stored messages

4.1 Investigating ICQ

All my tests were performed in the security lab at Blekinge Institute of Technology. In my tests I used six computers placed below a firewall and the computer layout was the following:

<table>
<thead>
<tr>
<th>Computer</th>
<th>Application</th>
<th>Operating system</th>
<th>2.nd operating system</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ICQ Pro 2003a</td>
<td>Windows XP</td>
<td>Not needed</td>
</tr>
<tr>
<td>2</td>
<td>ICQ Pro 2003a</td>
<td>Windows XP</td>
<td>Not needed</td>
</tr>
<tr>
<td>3</td>
<td>ICQ2Go</td>
<td>Windows XP</td>
<td>Windows XP</td>
</tr>
<tr>
<td>4</td>
<td>ICQ2Go</td>
<td>Windows XP</td>
<td>Windows XP</td>
</tr>
<tr>
<td>5</td>
<td>Licq</td>
<td>Red Hat 8.0</td>
<td>Not needed</td>
</tr>
<tr>
<td>6</td>
<td>Licq</td>
<td>Red Hat 8.0</td>
<td>Not needed</td>
</tr>
</tbody>
</table>

*Table 4.1, Overview of the laboratory environment*

In the security lab I used cloned installations of the operating system to ensure against different results on different computers due to different settings. When investigating ICQ2Go, Microsoft Windows XP was installed on two partitions. When using an operating system, many system files are locked, which means you cannot create MD5 checksums for these files. However, if you boot on another installation, you will have full access to the investigated system and checksums can be created.

In this environment I had total control of the content of the disks and changes were monitored, but I could only investigate files on the hard disk. Erased files, RAM, cache etc. where not investigated due to the environment.

To investigate ICQ on Windows I used the applications WinDump, Ethereal, MD5summer, and icq2xml. For examining Linux, I used tcpdump and the function md5Sum. For comparing MD5 checksums from both platforms, I used the application MD5Sum verifier.
4.1.1 tcpdump and WinDump

tcpdump and WinDump are used to sniff and monitor network traffic. tcpdump runs on Linux and WinDump runs on Microsoft Windows. They are started in a console and have several options to fit your purpose. I present the settings used in my tests in Appendix 1. When you have recorded your transmissions, you can analyze the traffic in Ethereal. The recorded traffic is stored in a dump file, so dump file in this report designates a file with network traffic made by tcpdump/WinDump.

4.1.2 Ethereal

Ethereal is an analyzing tool that allows you to examine packets from a dump file, by allowing you to browse network packets and see their content. I used Ethereal's latest version 0.9.8. When you have opened a dump file, you can browse through packets and look at their content. You will be able to extract everything from the packets including flags and data content.

![Ethereal Window](Figure 4.1, An Ethereal window)

4.1.3 MD5

To investigate if hidden evidence can be found on a system using ICQ, I calculated MD5 checksums on the examined drives. I used the application MD5summer v1.1.0.19 on Microsoft Windows XP. The application was written by Luke Pascoe and can be downloaded from [http://homepages.ihug.co.nz/~floydian/md5/](http://homepages.ihug.co.nz/~floydian/md5/).
On Red Hat Linux I used the function md5sum for collecting MD5 checksums. These were compared in my own developed application MD5Sum verifier which can be downloaded from http://www.student.bth.se/~is99ml/master.

4.1.4 ICQ database to XML converter

To read ICQ Pro 2003a’s history file I used the application icqhst-0.91. It was developed by Dipl.-Ing. Erwin Aitenbichler, at the Darmstadt University in Germany. Aitenbichler’s application extracts contacts and sent messages.

4.2 Workflow

To answer the questions posed, three tasks had to be carried out: the authentication phase, sending of messages, and viewing of the ICQ history.

4.2.1 Authentication phase

ICQ’s authentication phase was the first to be examined. I decided to create two ICQ accounts: Pepsi and Coke. As passwords, I chose words of different length and meaning. Pepsi received the password peppi and Coke the password cocacola. The following workflow was then performed once for each account and each of the three ICQ clients: ICQ Pro 2003a, Licq, and ICQ2Go.

Start WinDump
Authenticate to the ICQ network
Disable WinDump

I then analyzed dump files in Ethereal. ICQ starts its authentication process with a TCP handshake. The client first sends a SYN to the server which replies with SYN + ACK. The client then completes the handshake by sending an ACK package. After the completed handshake the server sends the packet SRV_HELLO. The next packet is the CLI_IDENT packet, which contains information about the client, including UIN, Password, ICQ version, language and country [McLaughlin, 2003]. The password is encrypted by using a XOR key. Melina claims the key to be F3, 26, 81, C4, 39, 86, DB, 92 and 71 in hexadecimal notation. [Melina, 2002] The maximum password length is eight and every character is always XOR:ed with the same piece of the key.

Hexadecimal notation and XOR

Hexadecimal means 16 and is a notation with 16 numbers. In hexadecimal notation four bits (1 or 0) represents one character. It starts to count from 0 (0000) and
continues up to 9, A represents ten and the last character is F (1111), which stands for 15.

XOR means *exclusive or* and is a Boolean operation that works at bit level. The following operations are available:

<table>
<thead>
<tr>
<th>XOR</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

*Table 4.2, Possible XOR operations*

To use Melina’s formula, you first need an encrypted password. In this example, I will use: 90, 47, EC, A1 and 55. The hexadecimal bytes in the table below have been written in the binary notation. The XOR operation is performed as follows:

<table>
<thead>
<tr>
<th>Password</th>
<th>1001 (9) 0000 (0)</th>
<th>0100 (4) 0111 (7)</th>
<th>1110 (E) 1100 (C)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key</td>
<td>1111 (F) 0011 (3)</td>
<td>0010 (2) 0110 (6)</td>
<td>1000 (8) 0001 (1)</td>
</tr>
<tr>
<td></td>
<td>0110 (6) 0011 (3)</td>
<td>0110 (6) 0001 (1)</td>
<td>0110 (6) 1101 (D)</td>
</tr>
</tbody>
</table>

*Table 4.3, Decrypting a password*

<table>
<thead>
<tr>
<th></th>
<th>1010 (A) 0001 (1)</th>
<th>0101 (5) 0101 (5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1100 (C)</td>
<td>0100 (4)</td>
<td>0011 (3) 1001 (9)</td>
</tr>
<tr>
<td>0110 (6)</td>
<td>0101 (5)</td>
<td>0110 (6) 1100 (C)</td>
</tr>
</tbody>
</table>

*Table 4.4, Continuing to decrypt the password from table 4.3*

In the bottom row, the bits 63, 61, 6D, 65, and 6C stand for camel in the ASCII table (Appendix 3); camel was the password decrypted by the XOR operation.

### 4.2.2 Messages

Sending of messages was performed by having all applications sending messages to all applications. Communication was therefore performed in all six different ways possible.

- ICQ Pro 2003a &gt; ICQ Pro 2003a
- ICQ Pro 2003a &lt; ICQ2Go
- ICQ Pro 2003a &lt; Licq
- ICQ2Go &gt; ICQ2Go
- ICQ2Go &lt; Licq
- Licq &gt; Licq

Before the communications, I created MD5 checksums of the hard drive. After the transmissions, a second round of MD5 checksums was taken for comparison.
In the first test, I sent four messages from each client. The messages were in a 
standardized form and had the same content. The content was as follows:
“Message 1”
“Reply Message 1”
And so on up to Message 4
I then went into direct chat mode (ICQ Pro 2003a and Licq) and continued the 
communication:
“Direct Message 1”
“Reply Direct Message 1”
And so on up to Direct Message 4

When analyzing the dump files, I looked at the following aspects:
Is the transmission in clear text?
Which protocol is used?
Which ports are used and are always the same ports used?
Where does the communication go?

4.2.3  ICQ history

ICQ Pro 2003a’s messages are stored in a database file (*.dat) on the local computer. 
The file also stores your contacts. If you have a “normal” hierarchy on your English 
based Windows system you should find the dat file at “C:\Program Files\ICQ\2003a” 
named “UIN”.dat, e.g. 230284085.dat.

The dat file is not in text-only format but uses parts text format and parts unknown 
format. The file is partly readable but you do not get all the information from it. You 
can see content of messages, but not when it was sent, or whom it was sent from or to.

To read ICQ Pro 2003a’s history file I used the application icqhist-0.91. It was 
developed by Dipl.-Ing. Erwin Aitenbichler, at Darmstadt University in Germany. 
Aitenbichler’s application extracts contacts and sent messages.

Since ICQ2Go does not have an installed application, it does not have a history file. 
To analyze ICQ2Go I took MD5 prints of the system. With this test, I investigated 
whether the use of ICQ2Go leaves any traces on the computer. ICQ2Go was only 
tested on Microsoft Windows systems.

Licq’s history file is in text format so I only attempted to interpret it. The time and 
date of messages are in a timestamp format and need to be translated. For this I used 
the simple perl script showed in figure 4.2.

![Figure 4.2, A perl script for translating timestamps](image-url)
5 RESULT

5.1 Authentication phase

<table>
<thead>
<tr>
<th></th>
<th>ICQ Pro 2003a</th>
<th>ICQ2Go</th>
<th>Licq</th>
</tr>
</thead>
<tbody>
<tr>
<td>Which port is used? (server-side)</td>
<td>5190</td>
<td>80</td>
<td>5190</td>
</tr>
<tr>
<td>Which protocol is used?</td>
<td>AIM</td>
<td>HTTP</td>
<td>AIM</td>
</tr>
<tr>
<td>Is the authentication packet easy to find in a dump file?</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Was the authentication packet secured?</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Table 5.1, Summary of the authentication phase

5.1.1 Analyzing the authentication phase

The passwords for ICQ Pro 2003a and Licq were easily found in the packet presented by Melina. The packet is sent with the AIM (Oscar) protocol and is given the info “New Connection” in Ethereal (see figure below). It is sent from a port around 1330 (ICQ Pro 2003a) and 32000 (Licq). The destination port is 5190.

Figure 5.1, Screen shot of the authentication packet (ICQ Pro 2003a) in Ethereal

Encrypted password extracted from the loginPepsi.dmp with Ethereal:
83 43 F1 B4 50

83 XOR F3 = 70
43 XOR 26 = 65
f1 XOR 81 = 70
b4 XOR C4 = 70
50 XOR 39 = 69

Decrypted password: peppi (70 65 70 70 69) which is correct.

The login packet for ICQ2Go is not easy to find due to the commonness of the packet type. The packet is sent with the HTTP protocol and is given the info “HTTP
Continuation” in Ethereal (see Figure 5.2 below). It is sent from a port around 1100 and is sent to the HTTP port 80.

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>0.752396</td>
<td>205.188.213.249</td>
<td>10.1.11.97</td>
<td>TCP</td>
<td>http &gt; kcp [AC</td>
</tr>
<tr>
<td>8</td>
<td>0.752436</td>
<td>10.1.11.97</td>
<td>205.188.213.249</td>
<td>HTTP</td>
<td>Authentication</td>
</tr>
</tbody>
</table>

*Figure 5.2, Screen shot of the authentication packet (ICQ2Go) in Ethereal*

In ICQ2Go, the password was not sent in hexadecimal notation but in hexadecimal figures stored in text format. This means that the hexadecimal 32 (2 in decimal) and 34 (4 in decimal) makes the hexadecimal 24. The encrypted password string from Ethereal was 32 34 30 63 31 33 35 66 33 64 and after translating them **24 0C 13 5F 3D** was left. When comparing this string with the string from the login with ICQ Pro 2003a the string does not match. This means that Melina’s key for decrypting the password does not work on ICQ2Go! But the problem was not difficult to solve. The key to use for ICQ2Go was easily deciphered and is 54 69 63 2F 54 6F 63 and 54. A description of how I deciphered the password can be found in Appendix 2.

The encryption was then performed with the new key for ICQ2Go:

- **24 XOR 54 = 70**
- **0C XOR 69 = 65**
- **13 XOR 63 = 70**
- **5F XOR 2F = 70**
- **3D XOR 54 = 69**

Decrypted password: peppi (70 65 70 70 69) which is correct.

The traffic of the authentication phase by ICQ Pro 2003a and Licq was easily readable in Ethereal and both passwords could be decrypted with the simple key published by Melina. They communicate with the Oscar protocol to port 5190 on the server, which makes the traffic easy to spot in a dump file.

The traffic from ICQ2Go was not encrypted with the technique and key provided by Melina, but I was able to decipher the encryption in just 15 minutes without the help of any decryption application. This shows how poor the used encryption algorithm is.

**In what way does ICQ secure your authentication process?**

ICQ uses a weak encryption algorithm for the protection of your authentication process. This makes the process unsecured. Your account can be hijacked and another person can impersonate you and send messages that you dislike.

**5.2 Messages**
5.2.1 Analyzing the messages phase

Both ICQ Pro 2003a and Licq use the same technique when sending messages. They start a transmission by sending the first messages through an ICQ server. They then continue the transmission peer-to-peer (p2p). The message sequence when transmitting through a server is easier to monitor than the p2p transmission since the server uses the IM specific AIM protocol. The p2p transmissions are sent over TCP, which is a more common protocol, and are therefore harder to locate in a dump file.

Even harder to read is communication generated in chat mode on ICQ Pro 2003a and Licq. In chat mode every character is sent in an individual TCP packet. This makes it more time consuming for an analyzer to retrieve information from the dump file.

ICQ2Go consumes the most of an analyzer’s time since it uses the HTTP protocol. The messages are sent precisely as web pages and are therefore hard to find. In a preliminary investigation, I got results different from laboratory investigations and other preliminary investigations. At that time, ICQ2Go used the SSL (Secure Sockets Layer) protocol for its transmissions. Although it communicated through SSL, no encryption was used.

Direct messages in chat mode are not stored in a history file. When a chat session is finished, you are asked if you want to store the chat session. If no has been chosen, then no traces of the messages can be found.

The traffic with the messages by ICQ Pro 2003a and Licq was easily readable in Ethereal. They communicate with the Oscar protocol to port 5190 on the server, which makes the traffic easy to spot in a dump file. But, after some messages, the protocol is changed to TCP and p2p techniques are used. This makes the analyzing harder and more time consuming for an investigator.

<table>
<thead>
<tr>
<th></th>
<th>ICQ Pro 2003a</th>
<th>ICQ2Go</th>
<th>Licq</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is the transmission in clear text?</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Which protocol is used?</td>
<td>AIM/TCP</td>
<td>HTTP/SSL</td>
<td>AIM/TCP</td>
</tr>
<tr>
<td>Where does the communication go?</td>
<td>Via server/Direct</td>
<td>Via Server</td>
<td>Via server/Direct</td>
</tr>
<tr>
<td>Which protocol and port is used? (server-side)</td>
<td>AIM-5190</td>
<td>80</td>
<td>AIM-5190</td>
</tr>
<tr>
<td>Which protocol is used? (p2p)</td>
<td>TCP</td>
<td>Not used</td>
<td>TCP</td>
</tr>
</tbody>
</table>

Table 5.2, Summary of the messages phase
In what way does ICQ secure your messages from wiretapping?

ICQ does not use any encryption algorithm for the protection of your messages. This makes the process unsecured. Someone can intercept your messages and read its content.

5.3 ICQ History

<table>
<thead>
<tr>
<th></th>
<th>ICQ Pro 2003a</th>
<th>ICQ2Go</th>
<th>Licq</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is there a history file?</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Is the history file in clear text?</td>
<td>No</td>
<td>*</td>
<td>Yes</td>
</tr>
<tr>
<td>Is the history file readable with the help of an application?</td>
<td>Yes</td>
<td>*</td>
<td>*</td>
</tr>
</tbody>
</table>

*Table 5.3, Summary of reading the ICQ history*

5.3.1 Analyzing the ICQ history

For ICQ Pro 2003a I used Erwin Aitenbichler’s application icq2xml with success. It managed to extract contacts and messages from the history file. With the messages you received time, date, and the complete content.

Since ICQ2Go is web based it does not use a history file. The content you can find on the computer does not reveal anything about the messages and you can only find traces in Window’s log files that an ICQ2Go session has taken place.

Licq uses a history file for each contact. The history file is in clear text and contains received and transmitted messages. Time and date were extracted with the perl script described in section 4.2.3.

In what way does ICQ secure your history file from forensic computing?

ICQ does not use any encryption algorithm for the protection of your history file. This makes the storing of the history unsecured. If your computer is compromised, all your previous messages on ICQ Pro 2003a and Licq can be read.
5.4 Results

The use of the instant messaging application ICQ results in non-secure sessions.

- ICQ uses a very weak encryption algorithm for the protection of your authentication process.
- No encryption secures your messages from wiretapping.
- ICQ Pro 2003a and Licq stores copies of messages on the local computer without any protection from encryption.

With the three sub questions examined and answered, the conclusion is that the use of ICQ results in non-secure IM sessions.
6 DISCUSSION

In this chapter, I will further discuss some important issues that arose while writing this report. Finally, I will also present some possibilities of future studies.

6.1 Validity and reliability of the investigation

The tests in this thesis were strictly performed, and made repeatedly on different occasions in a laboratory environment. The results should therefore be regarded as correct, for the default settings in ICQ. What traces ICQ2Go leaves on the computer could not be fully investigated. As a result of the delimitations, I only inspected known files. No page files, data in RAM or deleted files were investigated. This could influence the result.

6.2 ICQ security

In Chapter 1, I presented that 80% of the business users of instant messaging applications, declared that they have not heard of any restrictions in the use of IM software on their workplace. I also mentioned that 84% of the surveyed companies had employees using IM software. Do they know what they are doing? When you use IM applications for business use, a strong encryption technique must be used for the transmissions. Otherwise, business secrets can be revealed.

When you use a strong encryption algorithm on all messages, you automatically get the password, and the contents of messages encrypted. But not only ICQ’s traffic should be secured. The application must also live up to certain security principles. Most ICQ applications released are beta and alpha versions, and thus should not be considered bug free and stable.

In the scenario in Chapter 1, the cracker stole an account and obtained the contact list from the ICQ server. If she manually had to put the contacts back on the list, the contacts could have become suspicious. The feature to obtain the contact list over the Internet is great for the ICQ user. But if your account gets stolen the feature is disastrous since the cracker automatically receives your contact list, and can pretend to be you.
6.2.1 SSL and encryption?

ICQ2Go often uses the HTTP protocol, but at an investigation the SSL protocol was used. SSL is a much more secure protocol with encryption among other features. Consequently, it must be a better choice. Although, no encryption was used here, may the use of SSL indicate that SSL will be the future of ICQ2Go, and hopefully together with encryption. Implementing SSL with encryption would eliminate all the dangers with ICQ2Go mentioned in this thesis.

6.2.2 AOL and ICQ

America Online is one of the world's largest companies. The fact that AOL controls ICQ Inc. illusionizes ICQ users that ICQ is given appropriate financial help along with know-how and a strong brand name. ICQ Inc. and AOL are also very good at hiding ICQ's weaknesses from the public. People therefore consider ICQ a secure application. But it can also be the other way around. ICQ can remain insecure because of AOL's ownership.

ICQ is a free product that does not generate a lot of money for AOL. AOL, on the other hand, has other commercial IM products with encryption for business users that they charge for. Rumors indicate that AOL did not buy ICQ because of the application, but because of the huge customer database. Thus, AOL's interest in ICQ may not be to deliver the best product, but to obtain as much customer data as possible.

6.2.3 ICQ in the future

As easy as it is to recommend business users not to use ICQ, as hard is it to make a recommendation to the common public. Does the public care if messages can be wiretapped? We have had telephones since invented by A.G. Bell in 1876, but there have not been any complaints about the lack of encryption. Although there are some major differences, ICQ is easier to eavesdrop on than a telephone call, since all the equipment needed can be downloaded from the Internet, and a sniff attack can be launched from an ordinary home computer.

ICQ is a great piece of software if the security is disregarded, and people like to use it. I do not think common people will stop using ICQ because of this thesis, but it should be banned from all work places.
6.3 Future studies

It would be interesting to perform the tests in this thesis on other instant messaging applications. Then, comparisons could be made to how secure ICQ is in contrary to the other most used applications, e.g. Yahoo! Messenger, AOL Instant Messenger, and Microsoft’s .NET Messenger. One could also look at other security risks since instant messaging applications are subject to other attacks, such as buffer overflows, etc.
7 CONCLUSION

In this thesis, I have in laboratory tests sniffed and monitored the instant messaging application ICQ.

The police can use the knowledge found in this thesis when fighting crime since most of the techniques used in this thesis were unfamiliar to them. They now have tools to monitor, and intercept network traffic containing ICQ messages. They also have an application that can extract messages from an ICQ history file for use as digital evidence in court.

Since ICQ also can be used by crackers, the main conclusion for this thesis is that the use of ICQ does not result in secure instant messaging sessions since:

- The authentication process is poorly defended
- All messages are sent unencrypted over the Internet
- There is no protection for the history file

ICQ could have more protection since it is owned by AOL, one of the world largest companies. AOL should take control over ICQ Inc. and demand better security since good techniques, which are cheap and easy to use, exist for encryption.

ICQ should not be used in offices since it does not protect the user's integrity. I do not even recommend anyone using ICQ if the conversation is to be regarded as private and sensitive. All information on ICQ must be regarded as public, and if you do not consent to this, you should not use the application.

As a conclusion, I recommend business users not to use ICQ. Business secrets can be revealed to competitors. You can also be fooled, i.e. you cannot be certain that you speak to the person that you think. For the common public, I cannot make any recommendations. But ICQ users have to know the risks in order to be more suspicious. They have to know that the adage “do not thrust the Internet” also applies to ICQ.
8 REFERENCES


ISS Oscar, Login detected to OSCAR Instant Messaging server.  


McLaughlin Douglas. CLI_IDENT.  


ISBN: 0-13-016093-8

ISBN: 91-86656-68-6

APPENDIX 1

The following is the settings used when starting tcpdump/WinDump.

E.g. tcpdump -w login.dmp -s 0 not broadcast
     windump -w login.dmp -s 0 not broadcast

I want to save the network traffic to a file, for this the –w option is used followed by a filename e.g. –w login.dmp.

I want to be able to read messages in the packets; therefore the packets can not be cut of after the default 68 bytes. I instead use the -s gear with to specify the snaplen. If the snaplen is set to 0 then whole packets are captured.

Not broadcast, means what is says, no broadcast messages will be caught.

APPENDIX 2

How ICQ2Go’s password got cracked

All you need to make the crack is one dump file containing a known password.

Workflow

- Sniff the traffic while making a login to the ICQ network through ICQ2Go
- Locate the password in the dump file
- Run the XOR function on the known password
- Test the received encryption key on another account (can be skipped)

First I looked in the dump files from ICQ Pro 2003a, to find out where the password is located. When I found where it should be, I looked at the contents of the dump file at the particular place. I then saw that it was not in the same format as in ICQ Pro, but I saw that the hexadecimal numbers were in text form. I then extracted the hexadecimal numbers, and saw that they did not match against the key used for ICQ Pro. Since I knew the contents of the password I could make the XOR operation backwards to receive the encryption key instead of the password. To test the encryption key, I tested it on the other account that I used in the investigation and it worked.
APPENDIX 3

ASCII table
Numbers

<table>
<thead>
<tr>
<th>Text</th>
<th>ASCII</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>30</td>
</tr>
<tr>
<td>1</td>
<td>31</td>
</tr>
<tr>
<td>2</td>
<td>32</td>
</tr>
<tr>
<td>3</td>
<td>33</td>
</tr>
<tr>
<td>4</td>
<td>34</td>
</tr>
<tr>
<td>5</td>
<td>35</td>
</tr>
<tr>
<td>6</td>
<td>36</td>
</tr>
<tr>
<td>7</td>
<td>37</td>
</tr>
<tr>
<td>8</td>
<td>38</td>
</tr>
<tr>
<td>9</td>
<td>39</td>
</tr>
</tbody>
</table>

Characters

<table>
<thead>
<tr>
<th>Text</th>
<th>ASCII</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>41</td>
</tr>
<tr>
<td>B</td>
<td>42</td>
</tr>
<tr>
<td>C</td>
<td>43</td>
</tr>
<tr>
<td>D</td>
<td>44</td>
</tr>
<tr>
<td>E</td>
<td>45</td>
</tr>
<tr>
<td>F</td>
<td>46</td>
</tr>
<tr>
<td>G</td>
<td>47</td>
</tr>
<tr>
<td>H</td>
<td>48</td>
</tr>
<tr>
<td>I</td>
<td>49</td>
</tr>
<tr>
<td>J</td>
<td>4A</td>
</tr>
<tr>
<td>K</td>
<td>4B</td>
</tr>
<tr>
<td>L</td>
<td>4C</td>
</tr>
<tr>
<td>M</td>
<td>4D</td>
</tr>
<tr>
<td>N</td>
<td>4E</td>
</tr>
<tr>
<td>O</td>
<td>4F</td>
</tr>
<tr>
<td>P</td>
<td>50</td>
</tr>
<tr>
<td>Q</td>
<td>51</td>
</tr>
<tr>
<td>R</td>
<td>52</td>
</tr>
<tr>
<td>S</td>
<td>53</td>
</tr>
<tr>
<td>T</td>
<td>54</td>
</tr>
<tr>
<td>U</td>
<td>55</td>
</tr>
<tr>
<td>V</td>
<td>56</td>
</tr>
<tr>
<td>X</td>
<td>57</td>
</tr>
<tr>
<td>Y</td>
<td>58</td>
</tr>
<tr>
<td>Z</td>
<td>59</td>
</tr>
</tbody>
</table>

Characters

<table>
<thead>
<tr>
<th>Text</th>
<th>ASCII</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>61</td>
</tr>
<tr>
<td>b</td>
<td>62</td>
</tr>
<tr>
<td>c</td>
<td>63</td>
</tr>
<tr>
<td>d</td>
<td>64</td>
</tr>
<tr>
<td>e</td>
<td>65</td>
</tr>
<tr>
<td>f</td>
<td>66</td>
</tr>
<tr>
<td>g</td>
<td>67</td>
</tr>
<tr>
<td>h</td>
<td>68</td>
</tr>
<tr>
<td>i</td>
<td>69</td>
</tr>
<tr>
<td>j</td>
<td>6A</td>
</tr>
<tr>
<td>k</td>
<td>6B</td>
</tr>
<tr>
<td>l</td>
<td>6C</td>
</tr>
<tr>
<td>m</td>
<td>6D</td>
</tr>
<tr>
<td>n</td>
<td>6E</td>
</tr>
<tr>
<td>o</td>
<td>6F</td>
</tr>
<tr>
<td>p</td>
<td>70</td>
</tr>
<tr>
<td>q</td>
<td>71</td>
</tr>
<tr>
<td>r</td>
<td>72</td>
</tr>
<tr>
<td>s</td>
<td>73</td>
</tr>
<tr>
<td>t</td>
<td>74</td>
</tr>
<tr>
<td>u</td>
<td>75</td>
</tr>
<tr>
<td>v</td>
<td>76</td>
</tr>
<tr>
<td>x</td>
<td>77</td>
</tr>
<tr>
<td>y</td>
<td>78</td>
</tr>
<tr>
<td>z</td>
<td>79</td>
</tr>
</tbody>
</table>