C P R C
CANADIAN POLICE RESEARCH CENTRE

C C R P
CENTRE CANADIEN DE RECHERCHES POLICIÈRES

TR-02-2001
Evaluation of the Test Delivery of The Investigator's Guide to Internet Relay Chat

Sgt. Jamie Kerr
Canadian Police Research Centre

TECHNICAL REPORT
February, 2001

Submitted by:
Canadian Police Research Centre

NOTE: Further information about this report can be obtained by calling the CPRC information number (613) 998-6343

NOTA: Pour de plus ample renseignements veuillez communiquer avec le CCRP au (613) 998-6343

Executive Summary

The investigation of Internet software and its capabilities can be difficult and complex, even for a highly trained specialist. It is particularly mystifying for investigators who do not have this level of training or experience and who may not recognize the potential evidence which can be available.

The intention of this course was to familiarize investigators, who have little experience in this area, with one type of Internet software that is widely used by both the general public and the criminal element. The purpose of this course is to a basic understanding of how the Internet Relay Chat (IRC) software works and how investigations can be conducted. This course is not intended to provide the skills and knowledge necessary to conduct an actual investigations, simply an overview of what evidence might be uncovered and the investigational challenges these investigations present.

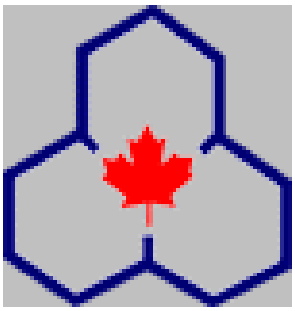
As little IRC Chat training developed with an investigative perspective is available, the CPRC intended to test the premise that inexpensive, reasonably comprehensive investigational training could be developed for this software which could then be delivered over the Internet. The evaluation of the first test course confirmed that such training could be developed and delivered inexpensively. The format of this training, which is highly interactive and uses IRC Chat software, was well received by the candidates. The draft course has been turned over to the Canadian Police College and has now been incorporated into their syllabus of courses which they provide over the Internet.

Sommaire

Les enquêtes menées sur le service Internet et sur ses capacités peuvent s'avérer difficiles et complexes, même pour un spécialiste qualifié. Ce genre d'enquêtes est particulièrement déconcertant pour les enquêteurs qui ne possèdent pas le niveau de formation ou d'expérience nécessaire et qui sont susceptibles de ne pas découvrir les preuves éventuelles.

L'objectif de ce cours consistait à familiariser les enquêteurs, qui ont peu d'expérience dans ce domaine avec un type de service Internet qui est très populaire auprès du grand public et des criminels. Ce cours a pour but de fournir des connaissances de base sur le fonctionnement du service de bavardage Internet Relay Chat (IRC) et sur la façon de mener les enquêtes. Ce cours n'est pas conçu pour fournir les aptitudes et les connaissances nécessaires pour mener des enquêtes, mais il donne un aperçu des preuves pouvant être découvertes et les défis relatifs à ces enquêtes.

Bien qu'il existe peu de programmes de formation sur le service IRC qui soient axés sur les enquêtes, le Centre canadien de recherches policières espérait démontrer qu'il était possible d'élaborer une formation complète et abordable axée sur les enquêtes relatives à ce service et de l'offrir sur Internet. L'évaluation du premier cours-pilote a confirmé la possibilité d'offrir une formation de ce genre à peu de frais. La structure de cette formation, qui est très interactive et qui repose sur l'utilisation du service IRC, a obtenu du succès auprès des participants. Le projet de cours a été présenté au Collège canadien de police et ce cours fait maintenant partie du programme de cours offerts sur Internet.



Evaluation of the Test Delivery of

The Investigator's Guide to Internet Relay Chat

Part of the Internet Skills for Law Enforcement Professionals Series
Developed by DM Toddington and Company

Delivered in partnership with

Canadian Police Research Centre
National Research Council Canada
Canadian Centre for Information Technology Security,
University of British Columbia
Northern Ontario Police Academy of Advance Training,
Cambrian College Sudbury
DM Toddington and Company

Course Coordination & Evaluation by

Sgt. Jamie Kerr
Canadian Police Research Centre

Report Contents

What is IRC Chat

While Internet 'chat' does not generally refer to actually speaking and hearing other people's voices, it does represent probably the most immediate way to communicate with others online via live, keyboard based 'conversations'. Using specially designed chat software, you type in words on your computer and other people in your 'chat room' can see what you are typing as you are typing it and vice versa. It is possible to hold many conversations simultaneously with different people located in many parts of the world and in different chat rooms.

While there are many different ways of chatting on the 'Net', the most popular method remains Internet Relay Chat or IRC. Of particular interest to the policing community, IRC can easily be used as a mechanism for like-minded persons to meet, discuss, plan and even engage in criminal activity. Well known for its use by pedophiles to exchange illicit pornography, numerous incidents have come to light recently in which sexual predators have used IRC to meet and lure away young victims. Organized groups known for promoting hatred frequently use IRC as a virtual meeting place for existing and potential new members, and extremist groups known for criminal behaviour are also strongly suspected of using IRC on a regular basis to communicate and further their goals. Further more, suspected criminal computer hackers can almost always be found online in IRC chat rooms freely discussing "how to" information and exchanging sophisticated "cracking" software and tools.

IRC follows a client-server model meaning that both client and server software are required to make use of it. While there are many IRC clients for many different types of computing systems[1], it is generally accepted that the most popular application is mIRC[2], developed as shareware[3] in the United Kingdom by Khaled Mardam-Bey. The focus of this training program, mIRC©, offers a generally intuitive interface for the first time IRC user while still allowing a significant amount of flexibility and capability for the advanced user.[4]

---

1 A cross section of IRC programs can be found at http://www.dragondate.com/toast/sofware.html.

2 mIRC is a registered trademark of mIRC Company Limited.

3 Shareware is software that is distributed free on a trial basis with the understanding that the user may need or want to pay for it later. Some software developers offer a shareware version of their program with a built-in expiration date (after which the user can no longer get access to the program). Shareware is sometimes offered with certain capabilities disable as an enticement to buy the complete version of the program.

4 Taken from the Introduction of "The Police Investigators's Guide to Internet Relay Chat", of the Internet Skills for Law Enforcement Professionals Training Series produced by DM Toddington and Company. Version 0.9 beta - January 1999.

Course Purpose

In recognition of the increasing emergence of Internet technologies in Police Investigations, The Investigator's Guide to Internet Relay Chat has been designed to promote a better understanding of IRC-based online communication from both a user's and an investigator's perspective.[5]

The course was designed to familiarize the candidates with the IRC Chat, its capabilities and complexities. The course was not designed to teach investigators how to conduct IRC Chat investigations - on the contrary - one of the purposes of the course is to demonstrate the technical and legal difficulties which must be overcome to conduct such an investigation. The material in this course suggests to the investigator that competent investigative assistance should be obtained before any IRC Chat investigation is undertaken.

Course Curriculum

This course is designed as an introduction to using the mIRC© Internet Relay chat program in a Windows 95/98 environment.[6] Emphasizing basic computer skills, this program is designed to be of value to experienced investigators who have had limited exposure to Internet technologies.

The Investigator's Guide to Internet Relay Chat consists of four individual lesson plans. Each lesson plan consists of self-study material and an interactive online session. Both the self-study and interactive components of each lesson plan will require approximately one hour each to complete (meaning a total of approximately 2 hours will be required to complete each lesson plan). Students will complete one Lesson Plan each week.

Live interactive sessions online with course instructors and other class members are designed to ensure that investigators gain exposure to computer technologies, develop new skills in the use of Internet communications programs and better understand key investigative techniques relevant to information technologies.[7]

---

5 Taken from the Course Introduction of "The Police Investigators's Guide to Internet Relay Chat", of the Internet Skills for Law Enforcement Professionals Training Series produced by DM Toddington and Company. Version 0.9 beta - January 1999.

6 Windows is a trademark of the Microsoft Corporation.

7 Taken from the Curriculum Introduction of "The Police Investigators's Guide to Internet Relay Chat", of the Internet Skills for Law Enforcement Professionals Training Series produced by DM Toddington and Company. Version 0.9 beta - January 1999.

Candidate Requirements

Candidates need only have access to the Internet via a Windows based computer on which they are able to install new software applications. They also will require the ability to send and receive Internet email and use a Web browser application.[8]

Candidates for this course should be experienced investigators working in an area where technological crimes may be uncovered. These candidates should also have a reasonably good working knowledge of Windows 95 or 98, Internet email and the World Wide Web.

Lesson One

This lesson shows how to locate, obtain, install and use this IRC Chat software.

Lesson One covers the following topics;

1. Downloading and installing the mIRC© software;
2. Launching and configuring the mIRC© program;
3. Selecting an IRC server and Network;
4. Logging on to IRC and joining a Chat channel; and
5. An overview of abbreviations frequently used on IRC Chat channels.

Lesson Two

This lesson shows how to access an IRC channel, private communication, file transfer, commands and command modes.

Lesson Two covers the following topics;

1. Obtaining a list of active channels from an IRC server;
2. Engaging in a private conversation online;
3. Using Direct Client Connection (DCC) to transfer a file to another IRC user;
4. Using manual IRC commands with mIRC; and
5. Various mode commands within mIRC..

[8] Taken from the Candidate Requirements of "The Police Investigators's Guide to Internet Relay Chat", of the Internet Skills for Law Enforcement Professionals Training Series produced by DM Toddington and Company. Version 0.9 beta - January 1999.

Lesson Three

This lesson gives an overview of IRC on the Internet, tracking, finding and identifying users with a variety of tools.

Lesson Three covers the following topics;

1. Introduction to the Internet and its architecture
2. An overview of Internet addresses;
3. Tracking IRC users with mIRC;
4. Using the WHOIS command;
5. Finding a User's Internet Providers (IP) address;
6. Client to Client Protocol (CTCP) queries; and
7. Tracking an IRC user through multiple IRC sessions.

Lesson Four

This lesson demonstrates a number of investigative tools as well as how to log communications and retrieve those logs.

Lesson Four covers the following topics;

1. Consolidating mIRC query tools and using UCENTRAL;
2. Logging IRC sessions and conversations; and
3. Retrieving LOG files.

Lesson Five

This lesson discusses a variety of legal considerations, limitations and powers which will affect an IRC Chat related investigation. Several recommendations and the investigators' criminal liability are also discussed.

Legal Considerations in IRC related investigations covers the following topics;

1. Logging mIRC chat sessions;
2. Interception of private communications;
3. Reasonable expectation of privacy; and
4. Judicial authority;
5. Standard search warrants;
6. Wiretap authorizations;
7. General warrants;
8. File transfers utilizing mIRC;
9. Legal recommendations; and
10. The criminal liability of investigators.

The Candidates

24 candidates were chosen from the agencies list below. Four candidates were from American law enforcement agencies, three from Canadian civilian agencies and the remainder from Canadian law enforcement agencies. Approximately half the candidates had extensive experience using and investigating IRC Chat matters, whereas the other half had no experience.

- Canadian Blood Services, Ottawa, Ontario
- Delta Police Services, Delta, British Columbia
- Edmonton Police Services, Edmonton, Alberta
- Military Police, Esquimalt, British Columbia
- National White Collar Crime Center, Fairmont, West Virginia
- Organized Crime Agency, Vancouver, British Columbia
- Ottawa Carleton Regional Police Services, Ottawa, Ontario
- Royal Canadian Mounted Police, Prince George, British Columbia
- SEARCH, Sacramento, California
- Specialized Computer Training, Canadian Police College, Ottawa
- Sudbury Regional Police Services, Sudbury, Ontario
- Telus Corporate Security, Vancouver, British Columbia
- University of Victoria, Victoria, British Columbia
- Victoria Police Services, Victoria, British Columbia
- Waterloo Regional Police Services, Waterloo, Ontario

The Instructors

The course instructors and moderators of the on-line IRC Chat sessions were David Toddington, Len Senetza and Stephen Thatcher. All are very experienced computer specialists actively involved in assisting various Canadian law enforcement agencies with complex computer and Internet investigations. Stephen Thatcher is a lawyer assigned to the 'E' Division Major Crime Section.

The Course Material

The 60 page course documentation and instructions, separated into the Four Lessons, were created using Adobe Acrobat and were downloaded by the candidates from the secure password protected course web site.

The Software

The software used was computer shareware called MIRC Chat which could be downloaded at no cost from the secure course web site.

On-Line Course Sessions

Four weekly live interactive course lessons were held with all candidates and instructors on January 18th, January 25th, February 1st and February 8th, 2000 from 1800 to 2100 PST. A password protected proprietary chat channel was used for each lesson, which only the course candidates and instructors could use.

Candidate Comments

1. This is a good introductory course which was easy to understand and improved the abilities of those not familiar with IRC Chat.
2. Excellent idea! Well executed - despite skill levels, time zones and hardware differences.
3. Felt at ease during the course. This was a good basic entry level course.
4. Good basic course. Excellent. Felt comfortable and got a lot out of it.
5. It helped tremendously. It did a great job of introducing IRC. Instructors were excellent.
6. Good enjoyable course.
7. Extremely well done.
8. The IRC format was excellent. Instructors did a great job. The handouts were easy to read and well put together.
9. Good helpful course. Interesting and the instruction was very good.

Candidate Suggestions

1. Teach the logging of chat conversations first, so that the candidates can log the on line sessions and have the option of going back over the lesson contents at their leisure.
2. Create small study groups of four or five candidates each and assign them a time to practice what they have learned. Maybe even setup a practice chat room on semi-permanent basis.
3. Include the complete IRC Chat help contents and a list of the common commands in the course handout. This would be really handy for the candidates to have in front of them as they go through the lessons.
4. Provide some recommendations for other sources of information on IRC Chat, such as web sites or books that would help the candidates strengthen and expand their knowledge. Pointers to Canadian case law would be very helpful.

5. Emphasize Digital Officer Safety so the candidates have a good understanding of what people can learn about them and any methods they can use to minimize their risk.
6. Long detailed explanations should be included in the printed course handout, not covered on the on line sessions. The on line sessions just aren't the correct medium - with the long delays between questions and answers.
7. Review the lesson objectives both before and after each on line session, and before any additional sessions for candidate study groups. They are well covered in the course handout - but having them reinforced would help.
8. While on line, instructors should use specific colours for their text so they are instantly recognizable. All candidates should use their real names, rather than handles, during the on line sessions to minimize confusion as to who is who.
9. The legal discussions were difficult to follow during the on line sessions. On line really isn't the medium for detailed discussions. Also, legal requirements are so often tied to jurisdictions and/or to the specific preferences of individual Crown Attorneys. Suggestions and case law relating to IRC Chat within the course handout would be very helpful though.
10. Cover 'splitting' in the course handout so that candidates are aware of the possibility of being unexpectedly disconnected from the server before it happens. Then they won't be so surprised, will know what has happened and be able to reconnect with less confusion on their part.
11. The uncontrolled conversations from many people at once can be a little hard to deal with for candidates new to IRC Chat. Although in most cases the humour added a great deal to the enjoyment of the course. A little more structure would make it easier to follow the proceedings.
12. Understanding the powers and capabilities of the Channel Operator would be beneficial.
13. Could you explain a couple of additional IRC points? I see sometimes where it says "females automatically get voiced" - what is that? Can netsplit hacking allow one to eavesdrop on private conversations? This would be nice to know even on a basic course.
14. Candidates should understand - up-front - that this is a basic entry level information course - not investigative training.

Coordinator's Comments

Having taken part, as a candidate, during all on-line sessions I believe the candidate's comments were both accurate and comprehensive. This course was an excellent "first try". It proved to be a very good introduction to IRC Chat and seemed to make all the candidates, who were new to this software, quite comfortable with its use, capabilities and commands. The candidates who were already experienced with the software also felt this was a good basic introduction. The course handouts were excellent, easy to understand, to follow and informative. The instructors were also very good - knowledgeable, patient and maintained control during the on-line sessions with a good sense of humour. Overall the course was a success because it was both informative and fun.

Coordinator's Recommendations

This course candidates made many valid comments and suggestions which I have commented on in my recommendations for future deliveries.

Although a number of ideas are being mentioned for possibly inclusion during the next delivery of this course, it does not mean that the course, as it is was, was not very successful. The course was well received by the candidates and I was impressed with both how well it covered the subject area and how much fun it was. I believe this is an excellent course, which will be of benefit and interest to our candidates. My recommendations are offered only as 'fine tuning' of an already successful course.

1. **Course & Candidate Organization** - This course encouraged candidates to use a 'throw away' email address, under an alias, through a provider such as Yahoo or Hotmail. Those aliases, added a good 'real world' perspective to the course during the tracing exercises and should be continued. Future IRC Chat candidates would find it easier to follow discussions and conversational threads if both candidates and instructors used their real names during on-line sessions, rather than screen aliases. It would also be helpful if the instructors used specific text colours, so that their input could be instantly recognized as soon as appeared on the screen.

2. **Logging of IRC Chat Sessions** - Teaching this capability early in the course would allow candidates to capture everything that is being said during the on-line sessions. Using the logs created they could review these pearls of wisdom, explanations, suggestions and hints prior to the next lesson. It would also give them additional practice in logging and a much better appreciation of why logging is mandatory during actual investigations.

3. **Candidate 'study groups'** - Small study groups of four to five candidates going off into their own Chat Rooms to practice, either before or after on-line sessions, would greatly increase candidate capabilities. Also, it would give all candidates the opportunity to act as a Chat Room Operator. Lesson objectives could be reinforced before each "study group" which could be followed by a short mandatory quiz similar to those used on the Basic and Intermediate Internet Searching Techniques courses.

4. **IRC Chat Help File** - Including the Help File and some of the more common commands within the course handout, possibly in a separate appendix, would allow the candidates to easily refer to this information when they are on-line and in their 'study groups', without having to switch screens between Help and IRC Chat.

5. **Additional resource information** - Having a small selection of resource sites and books, which provide additional and more detailed information on IRC Chat, would be helpful. Links to specific investigational information, especially case law cites would be a great benefit.

6. **Legal Considerations** - Detailed legal discussions are hard to hold productively within IRC Chat quickly scrolling screen. IRC is best used for conversations that are short and quick. Questions and answers about detailed legal points can be neither quick nor short and can result in long waiting times for the candidates as lengthy questions and their responses are typed onto the screen. Also, local case law and Crown Attorney preferences can dictate completely different courses of action for what appear to be similar situations - based entirely on what jurisdiction they take place in. Possibly the legal aspects could be more fully and more efficiently covered within the course handout. Reference locations for case law decisions or even news reports would be a benefit here. This section could also be followed by an on-line quiz to ensure that the candidates fully understand the major points.

7. **Digital Officer Safety** - Officer safety and investigational integrity are two extremely important concerns. All candidates should complete the course with a solid understanding of as many aspects of officer safety as possible. They should understand that the tools they are using to identify and trace suspects can just as easily be used against them. The candidates must also completely understand that this course is a basic introduction to IRC Chat and, by itself, does not impart sufficient training or knowledge for a candidate to be able to carry out an investigation dealing with IRC Chat. These points could also be reinforced in an on-line quiz.

8. **Course Size** -. It may be necessary to make several additional 'test' deliveries of this course before arriving at a completely finished product. The instructors of these future 'test' deliveries may want to limit the number of candidates so that it is easier for them to concentrate on content and delivery.