Chapter 25

A TRAINING TOOL FOR INTERNET CRIMES AGAINST CHILDREN CASES

S. Aggarwal, B. Breeden, P. Henry and J. Mulholland

Abstract The Internet has greatly increased the vulnerability of children to those who would commit crimes against them. In response to Internet Crimes Against Children (ICAC) legislation, law enforcement agencies have dedicated resources to educate the public of the threat, respond to ongoing attacks, and assist victims. A significant trend in the investigation of ICAC cases is the proactive masquerading of law enforcement agents as vulnerable prey in Internet forums. This approach has shown great promise, and agents who have mastered it possess valuable knowledge and skills that could assist others. The Predator and Prey Alert (PAPA) system, a hardware and software suite of tools, originally developed for proactive shadowing, assistance and direct manipulation of a cyberstalking victim's computer, shows potential as a proactive forensic tool for ICAC investigations. This paper discusses the use of PAPA as a networked application to train law enforcement agents to investigate online cases involving the exploitation of children and teenagers.

Keywords: Proactive investigations, investigator training, Internet Crimes Against Children (ICAC) cases

1. Introduction

The Internet has greatly increased the free flow of information, overcoming many of the obstacles, e.g., culture, distance and time, that have kept people apart. Connectivity has become a two-edged sword, especially for the most vulnerable in society [9]. Increasing numbers of children are going online to learn, play and communicate with their friends [9]. In the past, child predators pursued children in public places; now they prowl online forums (chatrooms, peer-to-peer file sharing networks and gaming sites) looking for prey. The Office for Victims of Crime reports that teens, who are rebelling from parental authority or

Please use the following format when citing this chapter:

Aggarwal, S., Breeden, B., Henry, P., Mulholland, J., 2006 in International Federation for Information Processing, Volume 222, Advances in Digital Forensics II, eds. Olivier, M., Shenoi, S., (Boston: Springer), pp. 317–330.

dealing with issues of sexual identity, are especially susceptible to solicitations by Internet predators [3]. Internet Crimes Against Children (ICAC) include diverse offenses: attempted and consummated sexual assaults, illegal use of the Internet to transmit sexual material, direct solicitation of minors, and the production, possession and distribution of child pornography. ICAC crimes have several distinctive features [15]:

- Physical contact between the child and the perpetrator need not take place for victimization to occur.
- Repeated, long-term victimization may occur without the victim's knowledge. For example, sexually explicit photographs of children, once in the hands of child pornographers, often remain in circulation on the Internet indefinitely.
- Internet crimes transcend jurisdictional boundaries.
- According recent studies [3, 4], children may not realize that they have been victimized. Even if they do, they are not likely to disclose what happened.

Wolak, *et al.* [16] note that ICAC cases fall into three categories: (i) identified victims, (ii) undercover operations in which no child victims are involved, and (iii) child pornography. Only a fraction of ICAC incidents are reported to the authorities, e.g., law enforcement, Internet service providers, parents or children's hotlines [3]. As Medaris and Girouard [9] observe, "the Internet is a nearly perfect medium for offenders seeking children for sex. It provides privacy, anonymity and a virtually unlimited pool of unsupervised children and teenagers who may be susceptible to manipulation."

Nevertheless, as Mitchell, *et al.* [10] aptly point out, "this same anonymity is an advantage to law enforcement because it allows a 40-year-old investigator to go online posing as a 14-year-old girl. This permits law enforcement to be proactive in investigations in ways they previously could not, and it allows them to detect some offenders before they victimize an actual child."

The global reach and anonymity provided by the emergence of collaborative applications on the Internet have increased the scale and scope of ICAC cases [5]. Pedophiles currently use the Internet to :

- Establish instant worldwide access to potential child victims or other predators.
- Discuss their sexual desires openly.
- Share ideas about ways to lure victims.

- Provide mutual support of their adult-child sex philosophies.
- Assume disguised identities for approaching children.
- Participate in "teen chat rooms" to find out how and whom to target as potential victims.
- Identify and track down home contact information.
- Build long-term virtual relationships with potential victims [9].

Because of the vast number of Internet users, pedophiles easily find victims, and because of the cross-jurisdictional range of the Internet's reach, offenders face little risk of interdiction. A U.S. Department of Justice (DoJ) report [15] notes that the Internet is being used by predators to contact children and/or teenagers for the purpose of engaging them in sexual acts. The Internet is also used to produce, manufacture and distribute child pornography. Young people are constantly being encouraged to engage in and exchange pornography.

According to Medaris and Girouard [9], "[p]ornography is used to break down inhibitions and validate sex between children and adults as normal, and it enables the offender to have power over the victim throughout the molestation. When the offender loses interest, pictures of the victim are often used as blackmail to ensure the child's silence, and when these pictures are posted on the Internet, they become an enduring and irretrievable record of the victimization and a relentless, shame-inducing violation of that child's privacy."

Also, the Internet is being used to entice and exploit children with respect to sexual tourism, i.e., travel—with the intent to engage in sexual behavior—that is used either for commercial gain or personal gratification. This type of offender is not only willing to invest considerable time and effort to befriend and disarm a child, he is willing to cross jurisdictional boundaries. According to a DoJ report [3], "perpetrators travel hundreds of miles to different states and countries to engage in sexual acts with children they met over the Internet. Many of these cases involve local, state, federal and international law enforcement entities in multiple jurisdictions."

Cases dealing with the exploitation of children for unlawful purposes have been steadily increasing [14], but the resources needed to investigate these cases have not kept pace because the investigation of ICAC cases places substantial burden on local law enforcement. Wolak, *et al.* [16] observe "[s]ince the mid-1990s ... developing technologies have forced law enforcement to confront situations not anticipated in criminal statutes, master technical advances, develop new investigative techniques, and

handle criminal cases that often span multiple jurisdictions." According to Mitchell, *et al.* [10], ICAC are "widespread, occurring throughout the criminal justice system; they are multi-jurisdictional [and] so require extensive collaboration; they involve constantly changing technology; and they require specialized investigation methods."

2. Proactive Investigations

In response to the growing challenges of online crime, law enforcement has deployed innovative techniques to combat ICAC perpetrators. Foremost among these are proactive investigations that involve law enforcement agents posing as minors, lurking in chatrooms, and waiting to be contacted by offenders seeking underage victims [7].

Law enforcement agents at all levels are conducting proactive investigations for several reasons, including increased public safety, relatively low cost and administrative ease, and the potential to stop or apprehend criminals before they can harm innocent persons [15]. Although the agents pose as entities other than themselves, this activity is not considered entrapment if agents wait for suspects to make clear statements demonstrating a predisposition to commit a crime [14]. No minors are involved in these types of cases, but because of the anonymity of online forums, suspects believe they are communicating with minors. As such, the cases are referred to as "proactive" because they allow law enforcement to act without waiting for an offender to commit a crime against a juvenile victim.

According to Mitchell, *et al.* [10], proactive cases represent 25% of all arrests for Internet sex crimes against minors. Despite the advantages of proactive investigations, given the large number of law enforcement agencies, many with limited sworn officers, it remains a significant temporal and monetary burden to train and deploy agents in these investigations. For law enforcement to effectively track, arrest and gather evidence of ICAC incidents, they must be well-versed in computers and the Internet, the online social behavior of young people and suspects, and relevant investigative techniques [2]. ICAC cases and the agencies that respond to them require financial resources to acquire, maintain and upgrade equipment, maintain staff with expertise in computer technology, provide training in specialized investigation methods, and promote inter-jurisdictional cooperation—all while technology and criminal techniques are becoming increasingly sophisticated. Ideally, ICAC investigations can stop crimes in progress; findings suggest that the Internet may allow law enforcement to act before a youth is victimized, gather solid evidence of offenses, and track offenders [2]. Mitchell, *et al.* [10] sug-

gest that offenders arrested in undercover investigations pose significant risks to young people: in 13% of undercover investigations, offenders were found to be concurrently committing similar crimes with juvenile victims leading to the identification of molested youth. In 41% of undercover investigations, offenders possessed child pornography, revealing additional criminal conduct [7]. The track record so far is good: proactive prosecution of ICAC cases has produced high rates of guilty pleas and low rates of dismissed and dropped cases.

3. Using PAPA as a Training Tool

Several law enforcement agencies have developed facilities for ICAC investigations and many agents have gained invaluable experience in proactive techniques. In the face of the widespread ICAC threat, it is desirable that they leverage their experience and expertise to fight this growing category of crime.

We argue that the Predator and Prey Alert (PAPA) system [1], a tool developed for cyberstalking cases, is well suited for ICAC cases. The core PAPA system is a set of integrated tools originally designed to support agencies in helping victims of cyberstalking, facilitating the investigation of such crimes, and collecting, verifying and maintaining evidence for the subsequent prosecution of cyberstalkers. Not only can PAPA be adapted to proactive and reactive investigations, but it can also be deployed as an in-house or distributed training tool that can be used by expert agents to oversee and instruct inexperienced agents during ongoing investigations.

PAPA was designed with the following goals in mind:

- Permit agencies to remotely "shadow" a victim and provide assurance and advice when needed.
- Capture and log circumstantial data related to stalking activities so that an analyst can subsequently investigate and determine the identity of the predator.
- Capture evidence of probative value so that the suspect can be successfully prosecuted.

The PAPA architecture is illustrated in Figure 1. It is assumed that the expert agent has a primary communication channel with the predator via the Internet where he or she is working a case from home (this is standard practice in ICAC cases) [3]. Each time the investigating agent engages with the predator, say in an online game or in a chatroom, a session is established. A session used for evidentiary purposes begins

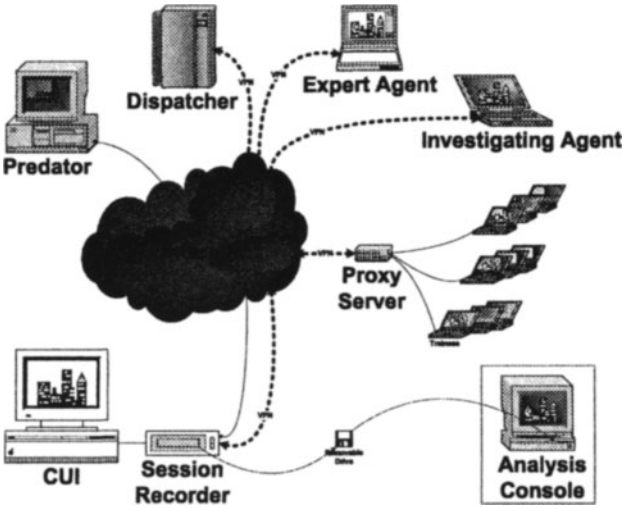

Figure 1. PAPA system architecture.

when the trainer agent logs in to guide the interactions between the predator and the investigating agent and endures until one of the parties logs out from the Computer Under Investigation (CUI). PAPA records the actual framebuffer content of the CUI during a session.

A hardware Session Recorder is connected to the CUI either through a USB or an Ethernet connection via LAN. This approach has several evidentiary advantages over collecting data directly on the CUI or sending video through slower channels. First, it minimizes modification of the CUI. Second, software-only solutions are potentially more insecure and susceptible to manipulation, and any evidence collected may become tainted. Third, it is much easier and less disruptive to transfer the large-capacity, dedicated disk from the Session Recorder to the Analysis Console while preserving the chain of custody. Fourth, private and sensitive data on the CUI that is irrelevant to the investigation is not compromised. Note that any solution that transmits captured video and other data to a remote storage location via the Internet may not be practical in low bandwidth environments.

PAPA keeps the management of captured data separate and independent of the other CUI functions. An independent second channel is used to communicate with the law enforcement expert (trainer agent). This channel could be a phone line, another high-speed Internet connection, Virtual Private Network (VPN), cellular, wireless, satellite, etc. Authorization and case coordination are achieved through communication

with the Dispatcher, which informs the expert when the investigating agent requests assistance, authenticates the agents' connections to the CUI via the Session Recorder, and continually monitors the state of the Session Recorder via a "heartbeat" protocol.

For completeness, PAPA captures all the video information from the framebuffer on the CUI. The high-speed connection permits the capture of video in raw mode, yielding a high-resolution image of activity on the CUI during the session. The Session Recorder also captures other meta information related to the session in the form of keystrokes and tagging of events. Video and metadata are time stamped, and metadata captured by filtering communications to the investigating agent's computer, such as IP header information and predetermined auxiliary textual and temporal information in the packet data, e.g., target words, screen names, email addresses and avatars, are also stored and used to index the video files. This indexing allows for rapid analysis of the potentially large evidence files.

The Session Recorder has a second logical channel between agents and the Dispatcher. This second channel is also secured using a VPN tunnel to conceal agent traffic from the predator, who communicates on the primary Internet connection channel and may have the ability to detect unusual traffic over the primary channel. If necessary, the second channel can be implemented over the primary connection. However, the investigating agent may lose bandwidth in the first channel and the predator may be able to detect traffic in the second channel.

The Session Recorder is connected to the Dispatcher to keep track of its status, and the Dispatcher also mediates all connections between the expert and the investigating agent. The channel between the agents operates transparently through the Session Recorder and all interactions can be viewed over the independent second channel. The channel between the agents is primarily implemented through a customized version of Virtual Network Computing (VNC) open source software [13]. VNC supports a variety of remote viewing and control modes between the remote desktop of the CUI and the agent. It requires a client running on the agent's computer (Agent Module), and a modified VNC server (Victim Module) running on the CUI. The VNC-based connection permits agents to view the investigating agent's screen and to take control of the CUI when necessary. PAPA implements an additional "chat channel" between the expert and the investigating agent to allow the expert to interact with the investigating agent independent of the communication between the investigating agent and the predator. This chat channel is also implemented through the independent second channel and the Session Recorder.

The PAPA system provides several features:

- Recording the user experience of the "victim," including all communications between agents, between the trainee and predator, and between the Session Recorder and the Dispatcher, in high-resolution, lossless and verifiable formats.
- Ensuring the integrity of evidence recorded by the Session Recorder via robust cryptographic hashing and access control mechanisms.
- Extending the evidentiary "chain of custody" from the CUI.
- Capturing all available evidence of the investigating agent's interactions during an online session, including relevant metadata such as time stamps and potentially relevant TCP/IP packet header and data information.
- Preventing all undetected pre- and post-computing of evidentiary data.
- Indexing suspected attacks and other incidents of interest within the potentially large video files created during a session.
- Coordinating network communications between the investigating agent's computer and law enforcement systems by means of an independent and secure second communications channel.
- Providing strong time-based verification of data reception, recording, and encryption through massive redundancy.
- Enabling flexible playback and queries of the online experience by both the agents to augment the learning experience.

This approach avoids the common issues of anonymity, lack of records and under-reporting inherent in computer crime cases. Furthermore, the predator's expectation of anonymity helps undercover agents monitor the predator's activities because the agents can assume the online identity of the victim to solicit further personal information and/or to set up a rendezvous with the predator.

4. PAPA Functionality

Hardware and software for recording video, audio and keystroke activity on the trainee's computer are currently feasible. This paper focuses on the ability to legally and contemporaneously record the activities involved in ICAC cases with the goal of gathering admissible electronic

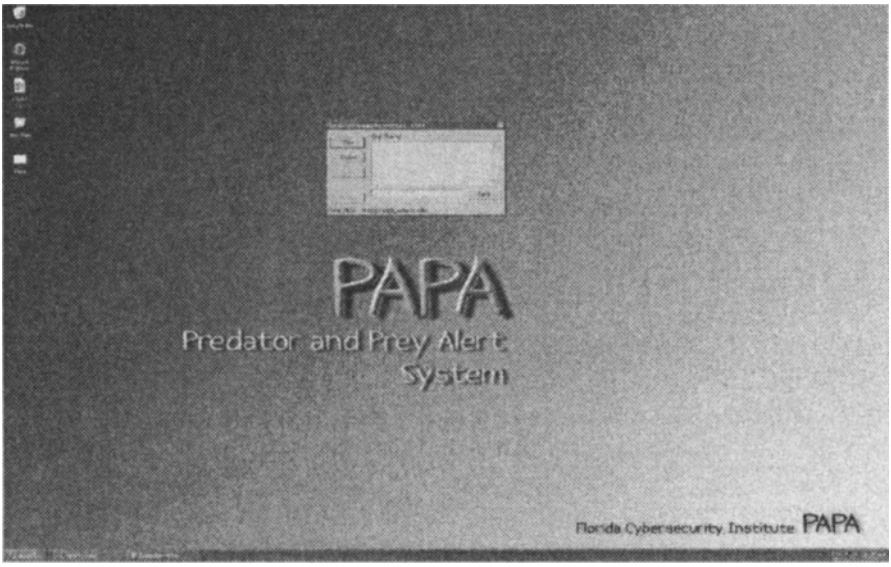

Figure 2. Expert Agent Module initialization.

evidence. All the PAPA features listed above have been designed with flexibility of deployment in mind. For example, the Session Recorder can be connected to the CUI in several ways, and the Dispatcher allows multiple agents in different locations to authenticate, log in, communicate and shadow the session.

Figure 2 shows the desktop of the Expert Agent Module, which features clients and their icons to initiate communication with the investigating agent. The initial chat dialog box is semi-transparent to allow monitoring of background windows. It always on top of the desktop so that incoming chat communication is visible. The box features buttons to view the CUI, control the CUI, tag incidents, stop the session and send messages to the CUI.

Figure 3 shows the desktop of the remote CUI and its contents in a window on the expert's computer. In this example, the CUI is running the popular game *World of Warcraft*, which demonstrates the graphic capabilities of PAPA. The game contains a fully functional chat room that is often a forum for predatory attacks. All the traffic between players is encrypted, which demonstrates PAPA's ability to do "insider" proactive investigations. In particular, note the lower video resolution within the window. The resolution is configurable from raw (full native resolution) to high levels of compression (Figure 3). This high level of compression

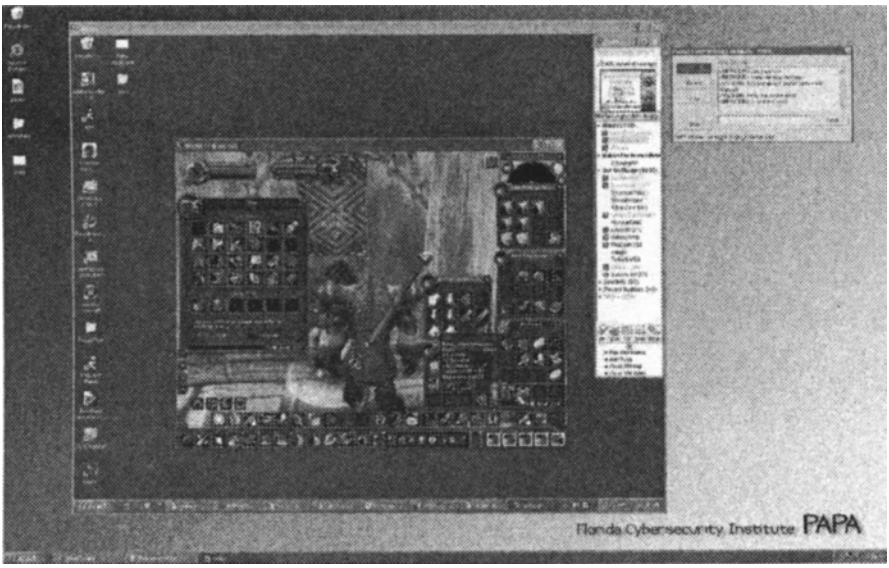

Figure 3. Expert Agent Module during a session.

allows for remote shadowing over low bandwidth connections, but comes at the cost of lower readability, stuttering screen refresh artifacts, and additional CPU load during signal compression and decoding.

Figure 4 shows the Expert Agent Module operating in View Mode, in which the agent can shadow (and record) the PAPA session. The expert may chat with the Investigating Agent Module via standard text entry, read messages from the CUI, and scroll through the dialog history. There is also the option of running PAPA in Control Mode, when the expert can preempt the local input of the CUI. Figure 4 shows a character in World of Warcraft stalking the investigating agent on the CUI. The attacker is "King Arabi" and he has typed: *"Why don't you call me? When can I see you again?"* in the game's chat box (lower left quadrant). The investigating agent notes that the attacker, who is not in "her" Friends List, has reappeared. The expert indicates that she sees the attacker too. At this point, the instructor guides the inexperienced agent through the session. Together, they engage the predator so that the investigating agent can solicit evidence for prosecution. In fact, agents being trained to work ICAC cases can view the entire sequence of events and discuss the effectiveness of various investigative techniques.

Figure 5 presents a view of the CUI desktop. It shows the Investigating Agent Module chatbox, which is moveable and semi-transparent.

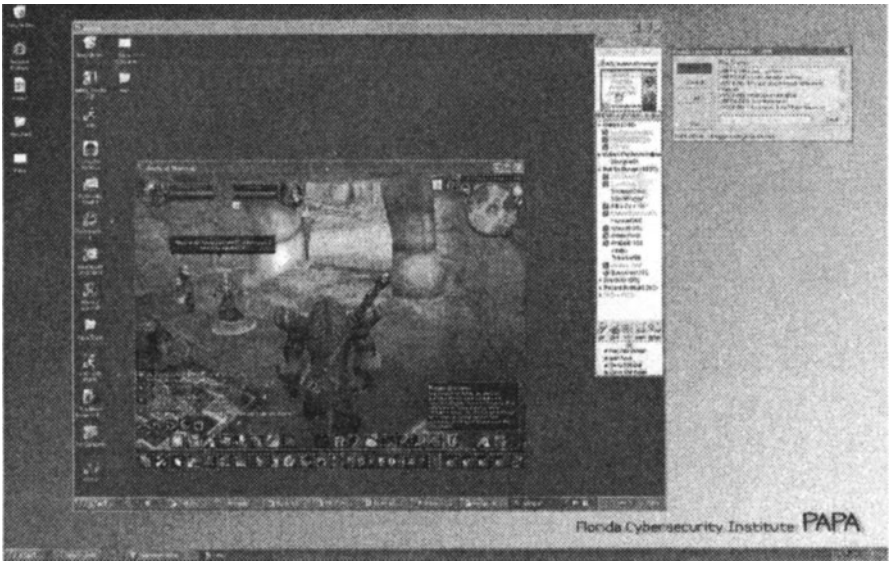

Figure 4. Evidence of a predatory attack.

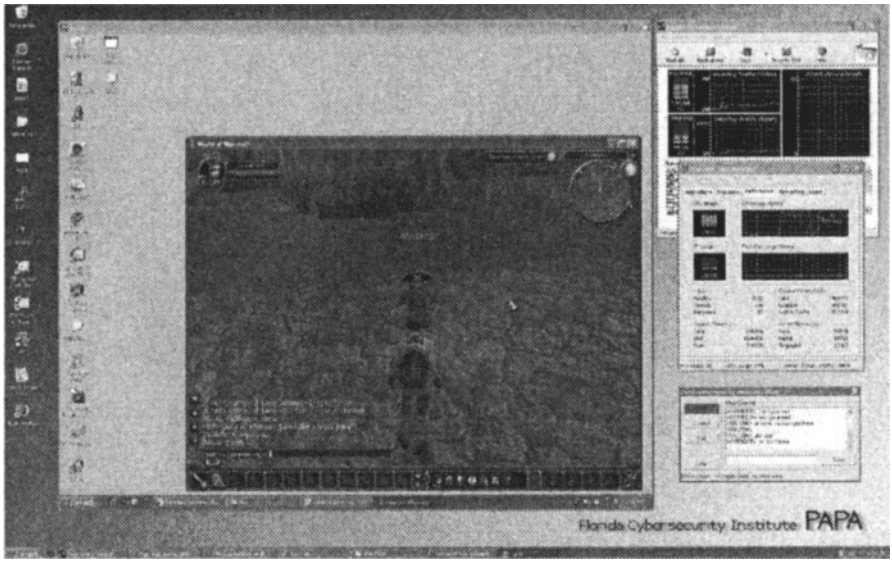

Figure 5. CUI desktop during an attack.

Figure 6. Expert Agent Module view of attack.

The chatbox buttons are Record, Tag, Stop and Send. It includes a scrollable dialog box that indicates that the session is being recorded. The *World of Warcraft* game is running in a window, and the chat between players is in the lower left corner.

Figure 6 shows the expert's view of the previous scene. Incoming and outgoing traffic are indicated in a Sygate Personal Firewall window, and memory and CPU load in the Windows Task Manager window.

PAPA can send the entire sequence to multiple law enforcement agencies to support remote training. For large-scale training applications it is desirable to operate PAPA in Proxy Mode, in which a proxy server is configured to relay the video. In this mode, PAPA can support higher resolution, switch between different host connections on the fly, enable reverse host connections, and accommodate hosts with variable desktop geometries.

VNC Reflector [13], a specialized VNC server, provides the ability to work with a large number of clients (viewers). However, if the signal is compressed to accommodate limited bandwidth, the viewing agents' computers must be fast enough to handle the overhead of decompression on the fly. Our experiments indicate that a 2+ GHz Pentium 4 machine with 1 GB RAM is sufficient for this purpose.

5. Conclusions

PAPA provides law enforcement agents with an understanding of proactive techniques used in ICAC investigations. It exposes trainees to advanced investigative techniques and protocols. Even more promising is PAPA's ability to leverage the behavior of an actual "gamer" as the CUI operator. The chat functionality provides support for the discourse between trainers and trainees, and is free of spatial constraints.

PAPA can be used for a variety of proactive investigations, including cases in which agents impersonate child pornography traders [3]. Also, it can support "reactive" or "take-over" investigations—when an officer goes online posing as a youth who has been solicited or as another youth. Furthermore, PAPA can support undercover operations that typically require covert, stand-alone phone lines or Internet access through non-government service providers [8].

PAPA is an effective training tool. Using the PAPA Session Recorder, experts can record, index and archive sessions for playback, self-paced learning and translation to other languages. PAPA helps agents and trainers overcome technical impediments in online child exploitation investigations. Also, it facilitates the rapid dissemination of new proactive investigation techniques.

Acknowledgements

This work was supported by the National Institute of Justice under Grant 2004-RD-CX-K154.

References

[1] S. Aggarwal, M. Burmester, P. Henry, L. Kermes and J. Mulholland, Anti-cyberstalking: The Predator and Prey Alert (PAPA) system, *Proceedings of the First International Workshop on Systematic Approaches to Digital Forensics Engineering*, pp. 195-205, 2005.

[2] S. Aggarwal, P. Henry, L. Kermes and J. Mulholland, Evidence handling in proactive cyberstalking investigations: The PAPA approach, *Proceedings of the First International Workshop on Systematic Approaches to Digital Forensics Engineering*, pp. 165-176, 2005.

[3] B. Breeden and J. Mulholland, Investigating Internet Crimes Against Children (ICAC) cases in the State of Florida, to appear in *Proceedings of the Twenty-First Annual ACM Symposium on Applied Computing*, 2006.

[4] D. Faulkner and D. Mahoney, Brief overview of pedophiles on the web (www.prevent-abuse-now.com/pedoweb.htm), 1997.

[5] D. Finkelhor, K. Mitchell and J. Wolak, *Online Victimization: A Report on the Nation's Youth - 2000*, National Center for Missing and Exploited Children, Washington, DC, 2000.

[6] Fox Valley Technical College, Protecting children online (www.missingkids.com/en_US/documents/pco_agenda.pdf), 2005.

[7] M. Girado, T. Deck and M. Morrison, Dissociative-type identity disturbances in undercover agents: Socio-cognitive factors behind false-identity appearances and reenactments, *Social Behavior and Personality*, vol. 30(7), pp. 631-644, 2002.

[8] ICAC Task Force, Training and Technical Assistance Program (www.icactraining.org/training.htm), 2005.

[9] M. Medaris and C. Girouard, Protecting Children in Cyberspace: The ICAC Task Force Program, NCJ 191213, Office of Justice Programs, Washington, DC (www.ncjrs.gov/html/ojjdp/jjbul2001_12_5/contents.html), 2002.

[10] K. Mitchell, J. Wolak and D. Finkelhor, Police posing as juveniles online to catch sex offenders: Is it working? *Sexual Abuse: A Journal of Research and Treatment*, vol. 17(3), 2005.

[11] National Center for Missing and Exploited Children, Alexandria, Virginia (www.ncmec.org), 2005.

[12] SourceForge.net, VNC reflector (sourceforge.net/projects/vnc-reflector), 2005.

[13] TightVNC Software, TightVNC (www.tightvnc.com), 2005.

[14] U.S. Department of Justice, Internet Crimes Against Children, NCJ 184931, Office for Victims of Crime, Washington, DC (www.ojp.usdoj.gov/ovc/publications/bulletins/internet_2_2001/internet_2_01.html), December 28, 2004.

[15] U.S. Department of Justice, Child victimization, *National Victim Assistance Academy Textbook*, Office for Victims of Crime, Washington, DC (www.ojp.usdoj.gov/ovc/assist/nvaa2002/toc.html), December 28, 2004.

[16] J. Wolak, K. Mitchell and D. Finkelhor, Internet sex crimes against minors: The response of law enforcement, National Center for Missing and Exploited Children, Alexandria, Virginia (www.missingkids.com/en_US/publications/NC132.pdf), 2003.