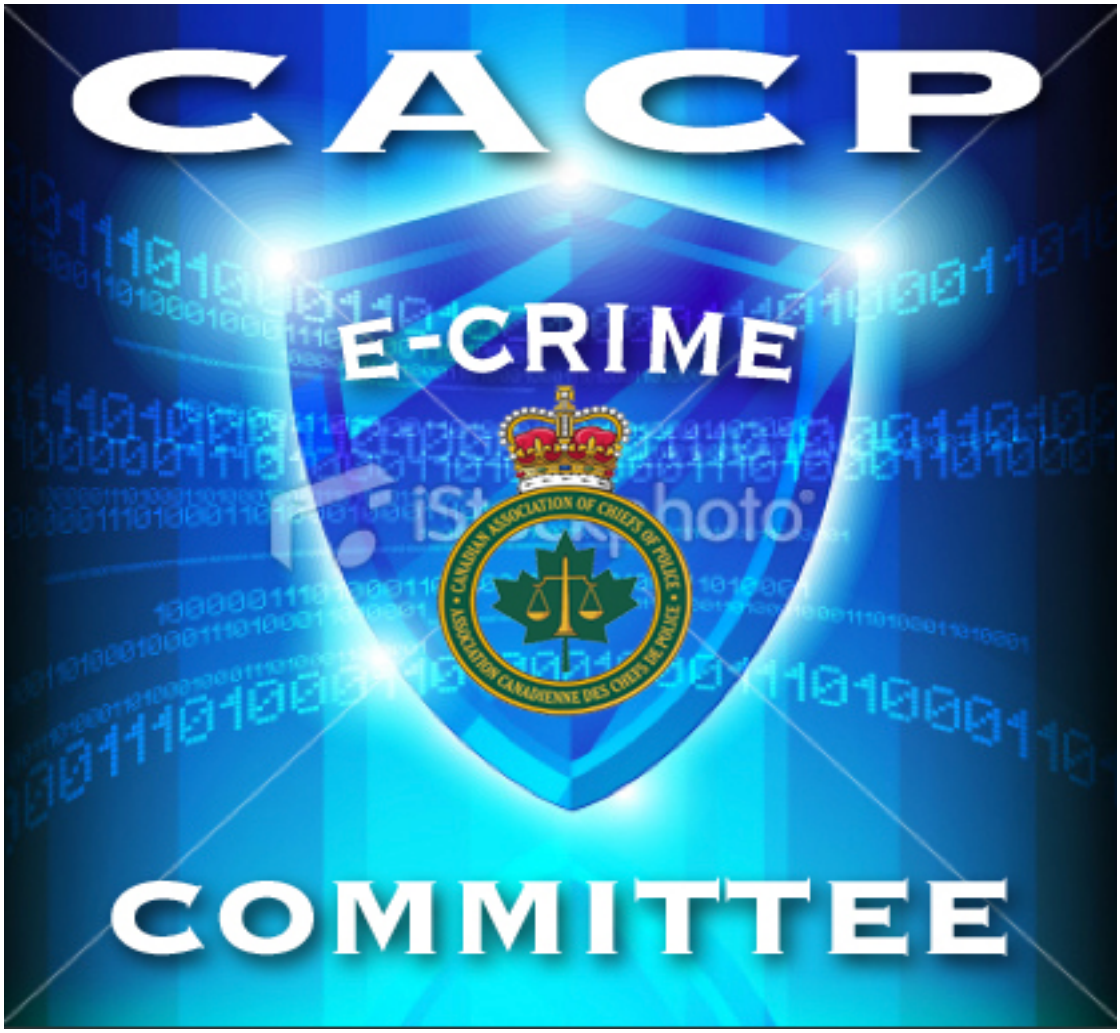
Canadian Association of Chiefs of Police Leading Progressive Change in Policing		**L'Association canadienne des chefs de police** À l'avant-garde du progrès policier

Electronic Crime Committee
2013 Annual Report



COMMITTEE MANDATE/OBJECTIVE

"To provide a national leadership role to the Canadian Law Enforcement Community on e-Crime related criminal investigations."

2013 MESSAGE FROM THE CO-CHAIRS

The Co-Chairs are pleased to present the 2012/13 CACP e-Crime Committee Activities Report on behalf of the Committee members who have worked diligently to achieve the goals and objectives set out at the beginning of our planning cycle. While the broader objectives of the Committee are aligned with the overarching goals and objectives of the CACP, the Committee also serves as a de facto community of practice for technological crime investigations.

In 2013, the Committee revised its mandate to better articulate its role within the CACP committee structure. The new e-Crime Committee mandate is…***to provide a national leadership role to the Canadian Law Enforcement Community on e-Crime related criminal investigations***. In keeping with this mandate statement, the report elaborates on a number of important initiatives that where undertaken this year and itemizes work planned for 2013/14.

In 2012, (CACP Resolution 2012-03) the e-Crime Committee proposed that the CACP champion the creation of a national cybercrime strategy. The e-Crime Committee, at its May 2013 meeting, presented a 'straw' strategy to stimulate discussion amongst the participants. Several police services indicated that they have been directed by their executive to engage on the issue of cybercrime making this initiative timely and relevant to the Canadian Policing Community. Since the May meeting, an ad hoc sub-committee has been formed under the CACP e-Crime Committee called the Cybercrime Consultative Group. The group's mandate is to examine training requirements for cybercrime investigators, look at the current investigative capacity across participating police agencies and best practices. This will feed the development of the broader national strategy.

Cybercrime, at the national and international level, is of strategic importance to the CACP as it relates to our primary role of advocating on behalf of law enforcement - policing. The interconnectivity of the world through the Internet to create cyberspace is changing the face of crime in Canada. The predominance of emerging criminal activities such as hacking, botnets, and malware have now become mainstream. Meanwhile, old crimes are being transformed. Money laundering is being facilitated through virtual worlds. Drug trafficking is made easier by orders placed on websites or contacts made via email or Twitter. The 21st Century bank robber uses today's technology to steal bank credentials removing the need to come through the front door with a loaded gun.

While technology is an enabler for organized crime there is, equally, a huge opportunity for law enforcement, as tools used by criminals become the source of valuable evidence. To this end, the e-Crime Committee advocates for a reasoned response to technological crime issues to government and police leaders while taking on practical initiatives to assist the broader community in this highly specialized area.

The Committee is composed of Canadian police leaders, private sector special advisors, justice experts and technical advisors. These members provide a vast array of knowledge and skills that position the committee well to achieve its objectives. The Committee membership includes police representatives from the RCMP, Ontario Provincial Police, Sûreté du Québec, as well as Toronto, Ottawa, Montreal, Saskatoon and Edmonton Police Services. Justice Canada and the Canadian Police College, who increasingly provide training efforts in this highly technical field, are also represented. The private and not for profit sectors are represented by the Canadian Bankers Association, Microsoft Canada and the Society for the Policing of Cyberspace.

The law enforcement members of the Committee thank our private sector members, not for profit society members and government partners for their continued participation, support and ongoing efforts in combating cybercrime. We recognize that there is a level of personal and professional commitment as well as the expenditure of financial resources which come with their participation. Going forward the Committee sees added value to including members of the academic community to the e-Crime Committee and will pursue this avenue over the coming year.

The Committee would like to acknowledge the outstanding contributions of past members Lieutenant Martin Charette, Co-Chair of the e-Crime Committee (2009-2012) Sûreté du Québec and S/Sgt. Marc Moreau (2006-2012) RCMP Technological Crime Branch. We wish you well in your future endeavors.

Superintendent Tony Pickett
Royal Canadian Mounted Police

Capitaine Frédérick Gaudreau
Sûreté du Québec

PROGRESS ON 2012/ 2013 INITIATIVES:

- **Hold regular Committee meetings, at least one in conjunction with other technology focused groups:** The e-Crime Committee held a meeting in October 2012 in conjunction with the Internet Corporation for Assigned Names and Numbers (ICANN) meeting held in Toronto. This provided a venue for Canadian Law Enforcement (LE) agencies to meet with International LE partners and discuss Internet Governance and its impact on criminal investigations.

- **Establish a recommended scientific methodology for the search, seizure and analysis of digital evidence:** The e-Crime Committee supports the establishment of a Digital Forensic Methodology (DFM). A Subject Matter Expert (SME) working group composed of SMEs from various Canadian LE agencies has been established. The group is in the process of modeling the DFM to a pre-existing International Standards Organization standard (ISO 27037). The work is continuing with the goal of completing a high level model for use within the Canadian LE community.

- **Examine the requirement for the validation of technical tools and utilities:** The e-Crime Committee continues to support the requirement for a validation component of tools used in the digital forensics process. The RCMP Digital Forensics Validation Team has refocused its mandate to better leverage validations completed by partner agencies and dealing with high risk activities and a tiered level of testing/validation. Tool validation is a component of the ISO 27037 being modeled in the course of the DFM.

- **Assess online training opportunities to reduce prohibitive training costs:** The e-Crime Committee has developed a unique partnership with Carnegie Mellon University, Pittsburgh, to provide cost effective training to all Canadian LE agencies and federal partner agencies. The program provides trademark Computer Emergency Response Training (CERT) online for a low yearly fee and provides training in various disciplines aimed at practitioners and managers.

- **Assess impact of Cloud computing in the scientific/forensic process and its foreseeable impact on court disclosure (reliability of seized data):** This issue will be addressed in the coming months through a proposed joint initiative between law enforcement and academia.

- **Assess impact of encryption on forensic examinations and due process:** The e-Crime Committee worked to respond to a survey for the Deputy Ministers of Justice and Public Safety (Federal/Provincial/Territorial), Coordinating Committee of Senior Officials (CCSO) Cybercrime Working Group (CWG). The CCSO CWG has since agreed that its work on the issue of encryption is no longer a viable option to addressing encryption related law enforcement obstacles, since the Government of Canada has already completed an extensive study. Therefore, there are no immediate plans for further work in this area. The issue remains an important subject matter to the law enforcement community and may need to be monitored for future developments.

- **Broaden committee membership (lacking Eastern Canada representation):** The e-Crime Committee has been steadfast in its resolve to increase geographic representation from across Canada. In July 2013, after a multi-year absence, a member of the committee has been identified from eastern Canada.

- **Identify opportunities for prevention and awareness:** The e-Crime Committee has supported the creation of a video lecture on Cyber Risks produced by Stark Productions. This is part of an overall series of short informative video episodes called S.M.A.R.T. Tips. In addition to this directed initiative, various Canadian LE agencies continued their usual outreach with the Canadian public to advise them of various cyber fraud schemes. Of particular note was a police ransomware scam that targeted Canadians. This malware locked their computer showing a pop-up window purporting to be from their local police or RCMP, accusing them of some illegal activity and demanding a fine be paid to unlock the computer. Police agencies across the country ensured appropriate public advisory messages were sent out to prevent additional victimization from this scam.

INITIATIVES PLANNED FOR 2013/ 2014:

- The CACP e-Crime Committee will support a Virtual Currencies Project (BitCoin). This multi-stakeholder project will analyze this new form of currency, specifically investigational issues in Canada.

- The CACP e-Crime Committee will support the development of an EnCase 7 software workshop allowing analysts to transition from previous versions of the computer forensics software.

- The e-Crime Committee will support continued work to develop a Digital Forensic Methodology to be used by the Canadian LE community. This initiative continues work initiated in 2012/13.

- The e-Crime Committee will support the work of a newly created sub-committee (Cybercrime Consultative Group) to examine and share best practices, educational opportunities, investigative information and other facets of cybercrime (pure computer crime).

- The e-Crime Committee will continue to support the development of a National Cybercrime Strategy.

- The e-Crime Committee will endeavour to form partnerships with Canadian academia, including Canadian universities, who have an interest in providing a safe cyber environment for all Canadians.

DATES/OVERVIEW OF MEETINGS

The e-Crime Committee meets in the fall to identify goals and objectives. Intersessionally, the Committee uses email and teleconferencing to further discuss objectives/initiatives and to determine an appropriate action plan for these items. A spring meeting is held to ensure action items have been addressed. The Committee members who participate in the meetings are supported by their respective organizations. CACP Board of Directors provides funds to offset certain expenses such as conference rooms and other logistical requirements.

Fall 2012
NTCAC & CACP E-Crime Committee Meeting
October 14th – 16th, 2012
Toronto, Ontario

The fall meeting of the CACP e-Crime committee and of the National Tech Crime Advisory Committee (NTCAC) was held in conjunction with a meeting of the Internet Corporation for Assigned Names and Numbers (ICANN) law enforcement and security day. This provided an opportunity for all attendees to participate in some of ICANN's activities in addition to their work with the NTCAC and CACP e-Crime committees. The below points outline the topics discussed during these 3 days:

- Discussion on the goals and objectives of the CACP e-Crime committee
- Overview was provided of ICANN's Security and Stability Advisory Committee.
- Overview of Virtual Worlds and their impact on criminality
- Overview of Drug Enforcement Agency investigations
- Overview of judicial order applications to be used with Internet Service Providers
- Overview of the Domain Name Service (DNS), DNS abuse, and common uses found for criminal domains and domain name registration basics.
- Presentation of a case study from the O.P.P.
- Overview and status of the American registry for Internet Numbers (ARIN)
- Overview of the International Domain Name variant project
- Overview of the Canadian Law Enforcement perspective
- Overview of Online pharmaceutical fraud
- Overview of the Canadian Cybercrime Strategy
- Overview of the Society for the Policing of Cyberspace (Polcyb)

Spring 2013
NTCAC & CACP E-Crime Committee Meeting
May 8th – 10th, 2013
Winnipeg, Manitoba

The spring meeting of the CACP e-Crime committee and of the National Tech Crime Advisory Committee (NTCAC) was held in Winnipeg. The below points outline the topics discussed during these 3 days:

- Discussion on the tech crime unit composition and strength for units across the country.
- Discussion on Universal Crime Reporting (UCR) codes and the possibility to create new codes to capture relevant e-Crime data and statistics.
- Discussion on search warrant applications relating to e-Crime.
- Presentation of a case study by the Calgary Police Service.
- Overview of the Digital Forensic Methodology project and upcoming steps.
- Discussion on validation of forensic tools and of the RCMP Digital Forensics Validation Team.
- Discussion on mainstreaming tools for use at the first responder level.
- Update to the online training with CERT at Carnegie Mellon University in Pittsburgh.
- Overview of the creation of a Cybercrime team within the Calgary PS.
- Overview of a Distributed Denial of Service (DDOS) incident against a Canadian bank.
- Overview of the discussions at the March 2013 CACP meetings.
- Discussion on redefined mandate and various potential initiatives for the coming year.

The e-Crime committee also held two teleconferences in conjunction with the NTCAC. The meetings were held in the spring and summer of 2013. The teleconferences served to finalize agenda items, discuss initiatives and solicit information for the completion of the yearly report.

Activities Planned/Significant Dates 2013/2014:

Aug 18th – 21st, 2013	Submission of 2013 Annual Report Annual CACP meeting Winnipeg, Manitoba
Oct 2nd – 4th, 2013	Committee Meeting Toronto, Ontario
Winter 2014	Committee Teleconference (approx. February)
Spring 2014	Committee Meeting (Location TBD)
Summer 2014	Annual CACP Meeting - TBD
Fall 2014	Committee Meeting (Location TBD)

CACP E-CRIME COMMITTEE MEMBERS LIST:

CACP Members

Tony PICKETT (Co-Chair)	RCMP Technical Investigation Services Operations
Frédéric GAUDREAU (Co-Chair)	Sûreté du Québec
Thomas FITZGERALD	Toronto Police Service
Grant FOSTER	Saskatoon Police Service
Ian KINGHAM	Ottawa Police Service
Garry MEADS	Edmonton Police Service
Bernard MURPHY	Ontario Public Prosecution Service

CACP Associate members

Ray ARCHER	Canadian Bankers Association
Bessie PANG	Society for the Policing of Cyberspace (Polcyb)
John WEIGELT	Microsoft Canada

Technical Advisors

Craig COUGHLAN (Chair NTCAC)	Calgary Police Service
France THIBODEAU	Canadian Police College
Dan MacRURY	Nova Scotia Public Prosecution Service
Carole MATTHEWS (Executive Secretary)	Ontario Provincial Police
Maurizio ROSA	RCMP Technical Investigative Services
Gareth SANSOM	Justice Canada

Success Stories 2013

The Prince County RCMP with the help of Major Crimes in P.E.I. conducted an investigation into a home invasion style robbery. A mobile device was seized in the course of this investigation and was analyzed by the RCMP H Division Integrated Tech Crime Unit (Halifax).

A conducted energy weapon was used in the course of the robbery and the male victim was kicked and punched. The victim was hospitalized for a broken nose, and for cuts and bruises to his face. One of the accused mistakenly pocket dialed his girlfriend during the robbery. Members seized her phone with consent and it was analyzed, verifying the incoming calls and her text messages. The analysis conducted revealed a total of 9 suspects were involved in planning and/or carrying out the robbery. The mobile device analysis also revealed who the main suspect was as well as his 8 accomplices and their role. The investigation culminated with the arrest and prosecution of these 9 suspects. The main accused pleaded guilty and was sentenced to 3 and half years in jail. The remaining 8 accused also pleaded guilty and were each sentenced to 2 years in jail as well as a fine.

The Internet Child Sexual Exploitation team of the Sûreté du Québec executed a search warrant at a male suspect's residence in assistance to the Peel Regional Police. The suspect had previously been arrested at the Toronto Pearson airport in possession of Child Pornography.

In the course of the analysis of the seized exhibits, a member of the Tech Crime Unit of the Sûreté determined that some of the computer files were encrypted using the "Dekart Private Disk" utility. The analyst also determined that the suspect used a complex personalized password system. Further analysis by this member allowed him to understand this system and subsequently discover a 27 character password created using keyword concatenation.

This member's perseverance allowed for the decryption of an Excel spreadsheet which contained an archived list of Child Pornography files. This process took 2 short weeks to achieve, as opposed to the several years it could have taken using conventional password defeating techniques. This very structured list provided content description of the child exploitation files, as well as the suspect's personal rating using a star system

The file analysis is still ongoing. This file has revealed the existence of several underage victims, the identification team of the Tech Crime Unit is assisting with victim identification. Of note, the suspect has travelled to 78 countries and possesses large amounts of material corroborating sexual assaults and production of Child Pornography. To date, as a result of the great collaboration between the Peel Regional Police and the Sûreté du Québec, 2 young victims have been identified.

Following a thorough national security criminal investigation named “Project STOIQUE”, the RCMP charged Sub-Lieut. Jeffrey Delisle with offenses under the Criminal Code and the Security of Information Act, which included breach of trust and communicating safeguarded information to a foreign entity without lawful authority.

Members of the RCMP Technological Crime Branch in Ottawa supported by National Division (Ottawa), B Division (St-Johns), 'C' Division (Montreal), H Division (Halifax), J Division (Fredericton), K Division (Edmonton) and O Division (London), and who worked on this case intensively for several months. This collaborative approach was paramount in obtaining timely analysis results, provided a great learning environment and became an incubator for the development of best practices. The computer forensics conducted on the hundreds of digital-related evidence seized during the course of the investigation corroborated the evidence obtained previously. The accused’s modus operandi was confirmed and revealed the extent of his activities.

The accused entered a guilty plea which marked the first time in Canada that an individual has been convicted under section 16. (1) of the Security of Information Act. DELISLE was sentenced to 20 years in prison for his acts of treachery.

The RCMP Technical Analysis Team (TAT), Ottawa, is a leader in advanced digital forensics in Canada, contributing to the administration of justice by offering specialized assistance to local, municipal, provincial, and federal law enforcement partners in Canada. As a recognized leader in BlackBerry forensics, TAT provides expert assistance to international partners and law enforcement agencies for high profile investigations. Over the past year, advanced research and development has expanded with investments made to support deep flash memory data recovery to address emerging technologies, as well as to repair damaged and broken devices.

Recent success stories from the past year include:

TAT assisted the Queensland Police in Australia on a murder investigation where the victim was executed and dragged into a river. The BlackBerry was water damaged and badly rusted necessitating extensive decontamination and hardware manipulation. Thanks to the hard work and perseverance of several dedicated people over several months, all of the data was successfully extracted. This resulted in crucial evidence being uncovered which in turn expanded the scope of the original investigation.

Assistance was provided to the Winnipeg Police Service as part of Project Flatlined, a joint RCMP/WPS investigation targeting the Hells Angels and its support club, Redlined. Hundreds of encrypted BlackBerry messages were processed by TAT, providing key evidence that ultimately increased prison sentences by 3 to 4 years for the key players, including the Manitoba Hells Angels president who received an 11 year sentence and surrendered over $500K in assets.

Following the stabbing death of a 23-year-old man by two young offenders, Ontario Provincial Police sought TAT's assistance to extract crucial evidence from one of the teen's locked BlackBerry device. According to the OPP analyst, who "was able to dump out a report for review and was walking the investigator through the data, [he] did a search on the first name of the victim and identified the deleted content; Investigator just about fell off her chair...!"

After a lengthy legal process, an Alberta trucker was found guilty of the March 2010 importation of 9 kilograms of cocaine and possession for the purposes of trafficking and given an 8 year sentence. Key evidence was extracted from two BlackBerry exhibits, establishing a compelling time line of the trucker's journey to California and back. The full Supreme Court of British Columbia judgment can be found under R. v. Pocasangre, 2012 BCSC 2040 (CanLII).

Timely BlackBerry analysis assistance was provided to the Ottawa Police Service in May 2013 to help with the final unsolved murder of 2012, the August drive-by shooting of a 22-year-old man in Blackburn Hamlet. Corroborating evidence was extracted from the BlackBerry and provided to OPS investigators. The following day, five arrests were made with the prime suspect being charged with first-degree murder, finally providing closure for family and friends of the victim.

In April 2012, Members of the National Division ITCU investigated a former House of Commons staffer who used its computers to stage a cyber-attack that shut down a Quebec government's website. Search warrants were executed at the House of Commons and computer forensics were conducted against several computers and related server logs. As these events occurred during the major students protests in the spring of 2012, the individual received house arrest for what a judge said was a crime and not political protest. Janvier Doyon-Tremblay, 29, pleaded guilty to using the computers to make data unavailable on the Quebec government server in the 2012 incident that made headlines across Canada. He was handed an eight-month conditional sentence and banned from using a computer except for work. "We are free to express ourselves in the free and democratic society we live in Canada," Judge David Wake said, calling the offence a "particularly serious matter."

In June 2012, a male was severely beaten outside a local Ottawa city bar and not expected to survive. The Ottawa Police Service obtained the surveillance video computer system possibly showing the suspect committing the beating. However, it was believed that the footage was erased purposely with the possibility of never recovering the video footage. The Ottawa Police Service's Computer Forensics Unit solicited assistance from the National Division RCMP (Ottawa), Integrated Technological Crime Unit (ITCU) in the recovery of the video that was crucial to the investigation. As the digital data appeared to be encrypted, using intensive techniques, research and persistence, the unit members successfully recovered the video, including footage clearly portraying a suspect committing the act, which was later identified by the local police. Based on the analysis of the recovered digital video footage, the suspect was arrested and charges were laid against the suspect. The matter is still pending in Court.

A 21 year old man was riding a Toronto Transit Commission (TTC) bus in Toronto and as he departed he was followed by the accused and an unknown male. In an attempt to murder the victim, the accused shot him three times at point blank range, hitting his neck, back, and hand. The attack left him a quadriplegic. At the time the accused was arrested, his cell phone was seized and sent to the Toronto Police Service Technological Crime Section for examination. Officers in this section found that the phone had been damaged and would not power on. Forensic investigators created a JTAG adaptor out of surplus electronics and recovered an incriminating conversation recorded on the phone. Although the gun was never recovered in this case, and the bullet fragments found could not identify the calibre of firearm, the victim described being shot with a black revolver. Found on the phone was a picture containing what appeared to be cash, drug paraphernalia, and a black revolver. The examining officers were able to obtain the EXIF data for this picture and testify that it was taken by a Nokia 6790, the same phone on which it was found in the possession of the accused.

Officers from the Toronto Police Technological Crime Section received an iPhone seized from a homicide investigation. This phone was password protected, encrypted and had been sent to two agencies for extraction but the phone could not be cracked. As a last resort the phone was sent to a US forensic company to have the actual memory chips dumped and extracted. Again the phone was returned and officers were advised the phone could not be cracked. Investigators from the Toronto Police Technological Crime Section applied a number of techniques in order to unlock the phone. By the end of the day they were able to crack the access code on the phone and extract all available data including pictures, Short Message Service (SMS), Multimedia Messaging Service (MMS), voice mails, and emails. The data was paramount to the investigation and assisted with the identification of those involved.

In March 2012, a vicious murder occurred at Pikangikum First Nation, in northern western Ontario. The investigation resulted in three males being charged with murder. In the course of the investigation search warrants were executed and five personal computers were seized and submitted for examination to the OPP Technological Crime Unit. The examination resulted in the recovery of incriminating communication between all three accused, both post and pre-offence. The examination also identified evidence of gang membership, which was believed to have been a motivating factor in this crime. The fact that numerous computers were found to contain similar findings assisted with the ability to validate the results; in particular in relation to the dates and times the communications took place. This was an important feature in regards to the credibility attributed to the findings, during court testimony. The findings associated to the computers were heard during one day of testimony on May 7th, 2013. All three accused pled guilty to 2nd degree murder on the morning of May 9th, 2013 and are awaiting sentencing.

In early June, a high value break-and-enter occurred in Central Ontario. The value in stolen property was in excess of $190,000.00. The victim's new Ford f150 was stolen at the same time. It was subsequently recovered in another part of the province. The vehicle was equipped with a navigation suite and when it was recovered the investigators contacted OPP Tech Crime Unit (TCU) to assist in recovering GPS data from the unit. The TCU examiner found little in the forensics community when he researched an extraction from a unit of this type until he reached out through a contact to Ford Motor Company in the United States. Our request was transferred to the Ford Motor Company of Canada (FOC) where their engineers assisted us in creating an VIN unique extraction tool specifically for the recovery of the data from this vehicle. The initial extraction recovered track logs from the vehicle to assist the investigative team. The assistance from FOC was covered under a production order obtained by the investigators. An extraction of this nature is unique and highlights the co-operation between industry and law enforcement. The investigation remains ongoing.

A suspect issued a warning message to a number of government and law enforcement agencies along with airline companies indicating there was an individual who was going to be flying into Canada aboard a passenger jet, and would use some means to destroy the plane. The warning message was eventually shown to be false, and originating from an Internet Cafe in the Greater Toronto Area. The cafe was located and the digital surveillance system was examined by members of the "O" Division ITCU (London). Still photos of the suspect were pulled out and the suspect was identified. The computers used by the subject were examined, and found to be reset by the program "DeepFreeze". In-depth analysis yielded the text of the message, artifacts from internet browsing history, and elements from "auto-type" and "auto-suggest" utilities that even showed the subject entering in search requests, typographical errors and all. This information was disclosed, prosecutors briefed, and faced with the evidence before him, the subject pleaded guilty to Terrorist Hoax charges and he was sentenced to 12 months jail time and a $20,000 restitution order.

The RCMP O Division ITCU (London) has been involved in an ongoing investigation into ransomware - malware that reports to its victims that they have committed a criminal offence, and a local police service is now demanding a fine payment by means of UKASH.

European law enforcement was investigating one strain of Ransomware, with assistance from various RCMP ITCU units across the country. In one instance an investigator from "O" Division ITCU received permission to take an image of one of the robot networks (BotNet's) servers - which turned out to be an embedded Linux-based system in a FM transmitter for a local radio station. The malware was located on the system and shared with the primary investigating agency to help further their efforts. The file is still under investigation.

The Saskatchewan Internet Child Exploitation Unit (Sask ICE), comprised of members from the Regina Police Service, Saskatoon Police Service, Prince Albert Police Service and RCMP, is an integrated unit that falls under the Criminal Investigations Division of the Regina Police Service. Sask ICE initiated Project FANABAS as a proactive undercover on-line initiative to identify child predator offenders looking to commit the offences of Luring Minors and the Exploitation of children through electronic files (images and/or videos) of Child Pornography, focusing on targets within Saskatchewan. ICE investigators made contact with possible targets using various “chat rooms” developed for and frequented by children. This proactive interaction resulted in several investigational leads being developed.

Operation SNAPSHOT was a multi-jurisdictional investigation involving ICE Units from Saskatchewan, Alberta, Manitoba, Nunavut and the Northwest Territories. The Operation was initiated through the National Child Exploitation Coordination Centre (NCECC) and ran from June 1, 2012 to Oct 10, 2012. The goal of the project was to focus on the most “prolific” offenders utilizing the various file sharing networks to possess and distribute Child Pornography. The various ICE Units executed 30 warrants in Alberta, Saskatchewan, Manitoba, the Northwest Territories and Nunavut. The Provincial Government recognized all of the Saskatchewan ICE Unit members at the Regina Legislative building on November 29, 2012, for this successful Operation and their continued work and commitment in this field.

Sask ICE has experienced great success in several other investigations involving suspects possessing Child Exploitation materials. Some of these investigations have been conducted in partnership with partner police agencies. Sask ICE has faced several technical hurdles involving encrypted data, sharing site restrictions and cloud computing issues. Sask ICE has achieved successful strides forward by taking a collaborative approach with the local Tech Crime Units, liaising with equipment manufacturers and service providers going so far as undertaking breakthrough technical solutions with the assistance of the RCMP Tech Crime Branch.
