FEDERAL BUREAU OF INVESTIGATION

Supervisory Special Agent (SSA)
Amanda J. Strickland
Cyber Division

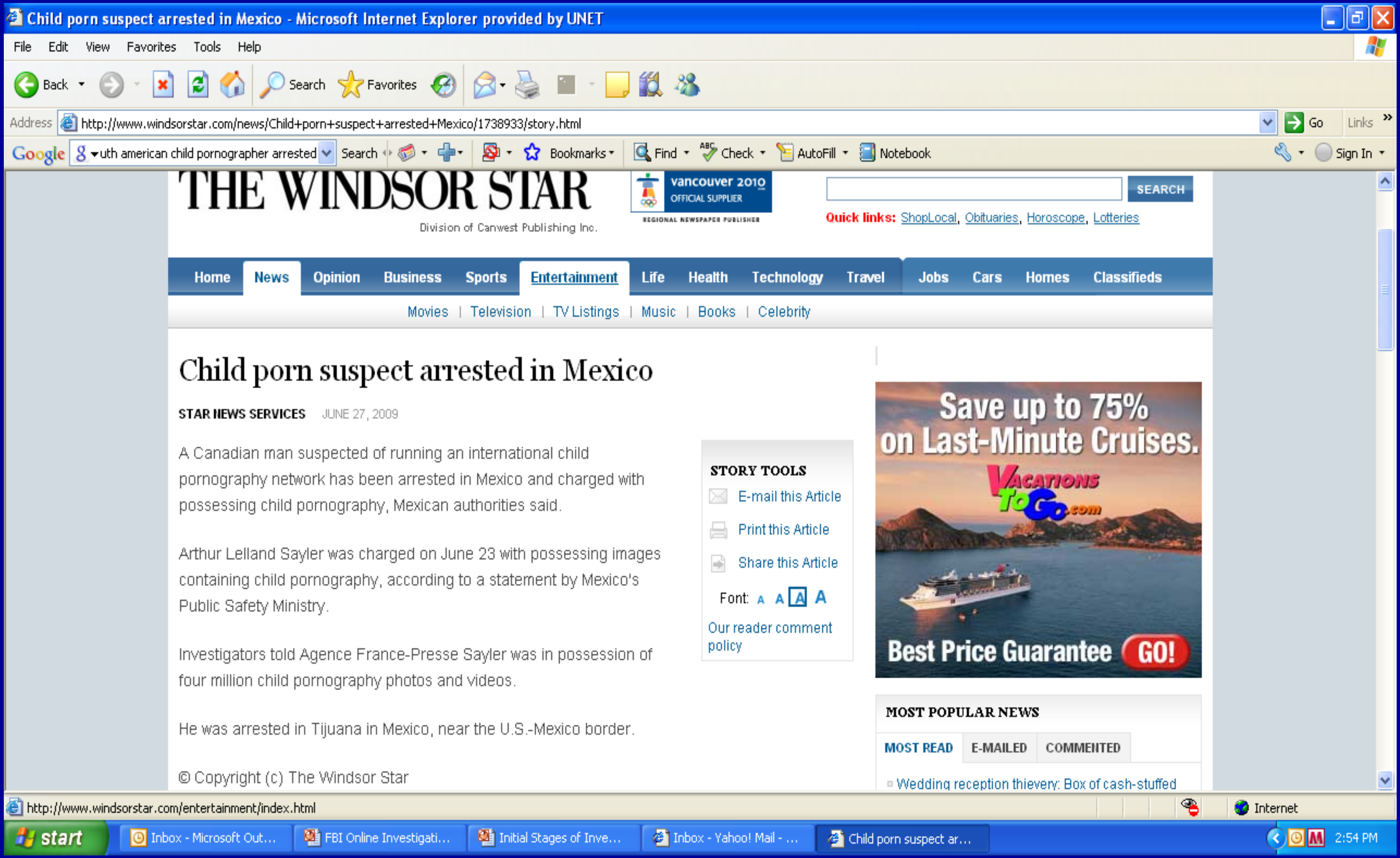
Initial Stages of Investigation

- Determine what approach to take.
- Identify the sources of electronic evidence
- Preserve electronic evidence
- Integrate electronic evidence into the investigation
- Case Management and investigation plan

Initial Stages of Investigation

- Perform traditional investigative steps:
  - Who, What, When, Where, how?
- Is there a victim? Is there a target?
- What crime has been committed? (fraud, intrusion, child exploitation, traditional crime)
    - Child exploitation/pornography cases are distinct from all others in the way they are initially approached by investigators.

Initial Stages of Investigation


Child porn suspect arrested in Mexico - Microsoft Internet Explorer provided by UNET
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.windsorstar.com/news/Child+porn+suspect+arrested+Mexico/1738933/story.html
Go Links
uth american child pornographer arrested Search Bookmarks Find Check AutoFill Notebook Sign In
THE WINDSOR STAR
Division of Canwest Publishing Inc.
vancouver 2010 OFFICIAL SUPPLIER
REGIONAL NEWSPAPER PUBLISHER
SEARCH
Quick links: ShopLocal, Obituaries, Horoscope, Lotteries
Home News Opinion Business Sports Entertainment Life Health Technology Travel Jobs Cars Homes Classifieds
Movies | Television | TV Listings | Music | Books | Celebrity
STORY TOOLS
E-mail this Article
Print this Article
Share this Article
Font: A A A A
Our reader comment policy
Save up to 75% on Last-Minute Cruises.
VacationsToGo.com
Best Price Guarantee GO!
MOST POPULAR NEWS
MOST READ E-MAILED COMMENTED
Wedding reception thievery: Box of cash-stuffed
http://www.windsorstar.com/entertainment/index.html
Internet
start
Inbox - Microsoft Out...
FBI Online Investigati...
Initial Stages of Inve...
Inbox - Yahoo! Mail - ...
Child porn suspect ar...
2:54 PM

Child porn suspect arrested in Mexico

STAR NEWS SERVICES JUNE 27, 2009

A Canadian man suspected of running an international child pornography network has been arrested in Mexico and charged with possessing child pornography, Mexican authorities said.

Arthur Lelland Sayler was charged on June 23 with possessing images containing child pornography, according to a statement by Mexico's Public Safety Ministry.

Investigators told Agence France-Presse Sayler was in possession of four million child pornography photos and videos.

He was arrested in Tijuana in Mexico, near the U.S.-Mexico border.

© Copyright (c) The Windsor Star

Initial Stages of Investigation

- Conduct your traditional criminal checks before leaving the building (+Search Engines)
- Systematic approach/Chaotic approach

Child Exploitation

- Conduct criminal history of checks for target or targets
- Determine who else has access to system
- Is there a possibility of imminent danger ?
- Possibility of Flight?
- Gather evidence
- Obtain legal authority to conduct searces
- Interview suspects

Property Intrusion

- What is the motive?
- Determine who has access
- Interview Systems Administrators and Other witnesses
- What is the purpose of the intrusion (theft/disruption)
- Internal vs External Threat

Fraud

- What is the fraud loss?
- Conduct criminal history of target or targets
- What type of fraud is being committed?
- What digital channels are being utilized to commit fraud
- How large is the fraud scheme?
- Possibility of Flight?

Traditional Types

- What type of crime was committed?
- What types of digital devices and services does the suspect use?
- Who has access to these devices and services
- Preservation of evidence

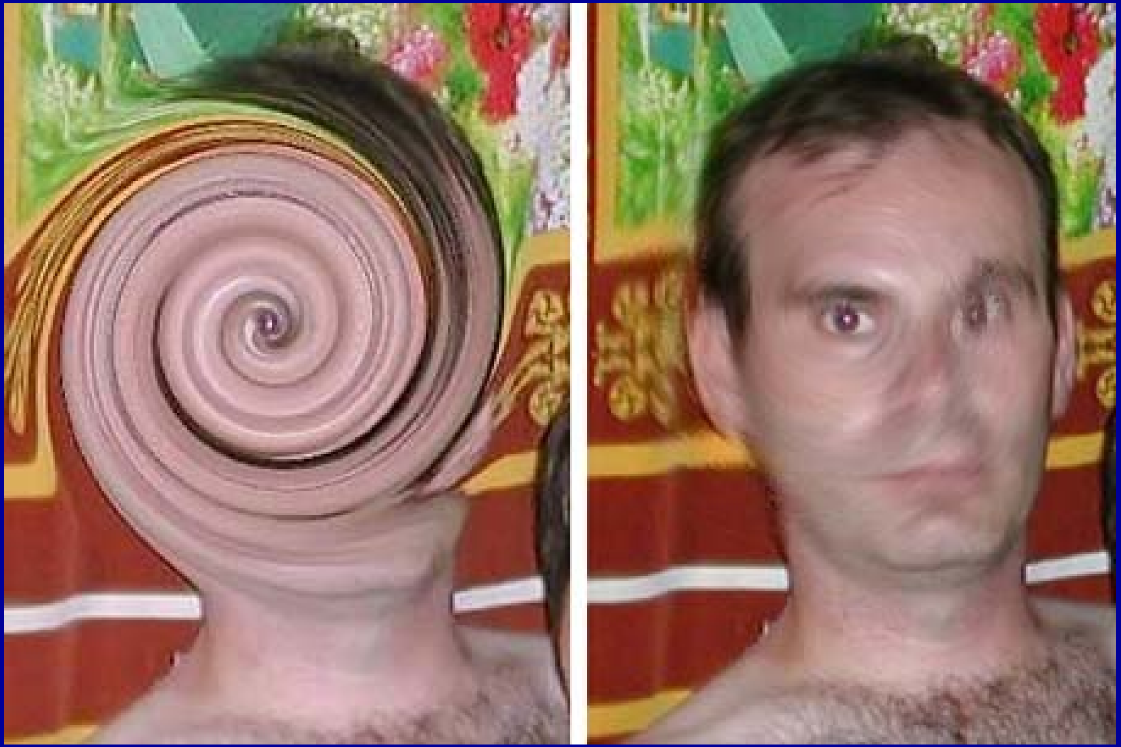
Sources of Evidence

- Divide evidence into 3 categories:
  - Host Based
  - Network Based
  - Other (Includes Interview information)

Host-based Evidence

- Child Exploitation
  - Email
  - Photo/Video
  - Documents
  - Chat logs

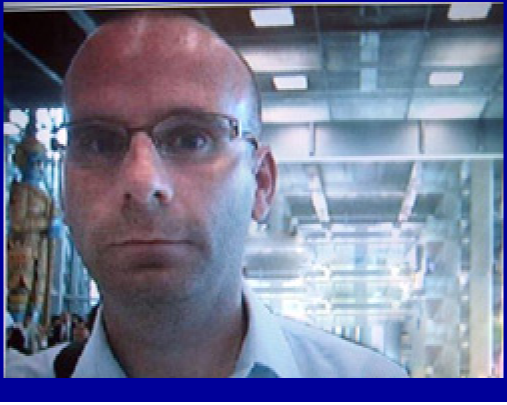
Interpol Case:
Christopher Paul Neil

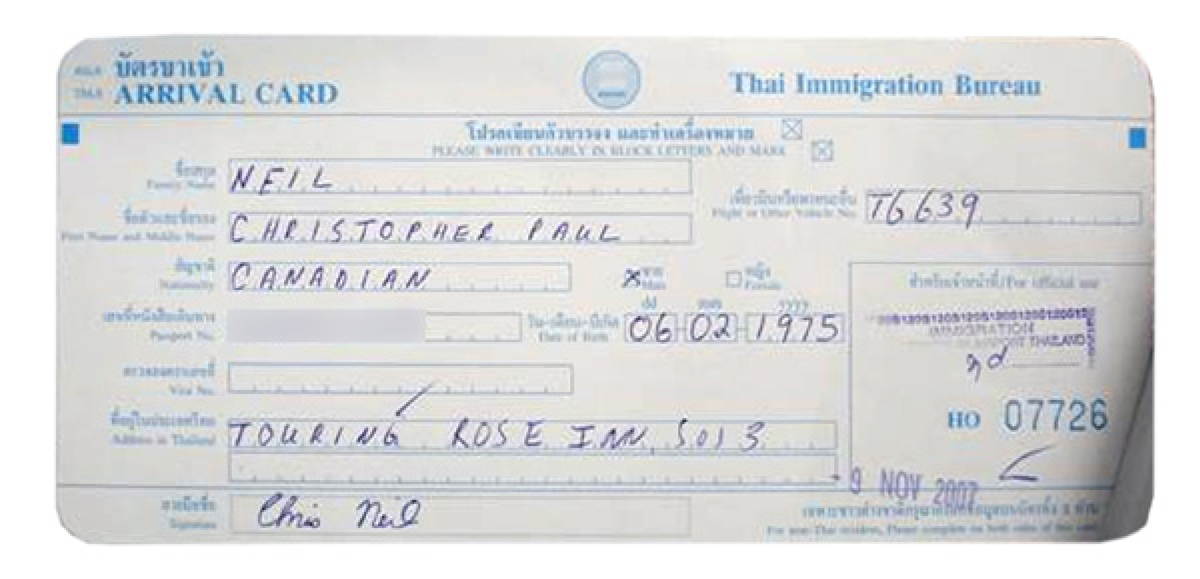


Interpol Case:
Christopher Paul Neil

- German police/computer experts “un-swirled” photo
- Interpol (circulated photo via Internet) received approximately 400 responses via email
  - Christopher Paul Neil
    - Taught English in South Korea
    - Three Thai youths contacted police after seeing Neil’s photograph on television. Neil showed them pornographic images on his computer.
    - Traced mobile phone calls made by Ohm, a 25-year old Thai transvestite Neil had befriended

Interpol Case:
Christopher Paul Neil





ตม.6 บัตรขาเข้า
TM.6 ARRIVAL CARD

Thai Immigration Bureau

โปรดเขียนตัวบรรจง และทำเครื่องหมาย ☒
PLEASE WRITE CLEARLY IN BLOCK LETTERS AND MARK ☒

ชื่อสกุล / Family Name: NEIL

ชื่อตัวและชื่อรอง / First Name and Middle Name: CHRISTOPHER PAUL

เที่ยวบินหรือพาหนะอื่น / Flight or Other Vehicle No.: TG639

สัญชาติ / Nationality: CANADIAN

☒ ชาย / Male ☐ หญิง / Female

เลขที่หนังสือเดินทาง / Passport No.: [redacted]

วัน-เดือน-ปีเกิด / Date of Birth: วัน 06 เดือน 02 ปี 1975

ตรวจลงตราเลขที่ / Visa No.:

ที่อยู่ในประเทศไทย / Address in Thailand: TOURING ROSE INN, SOI 3

ลายมือชื่อ / Signature: Chris Neil

สำหรับเจ้าหน้าที่/For official use

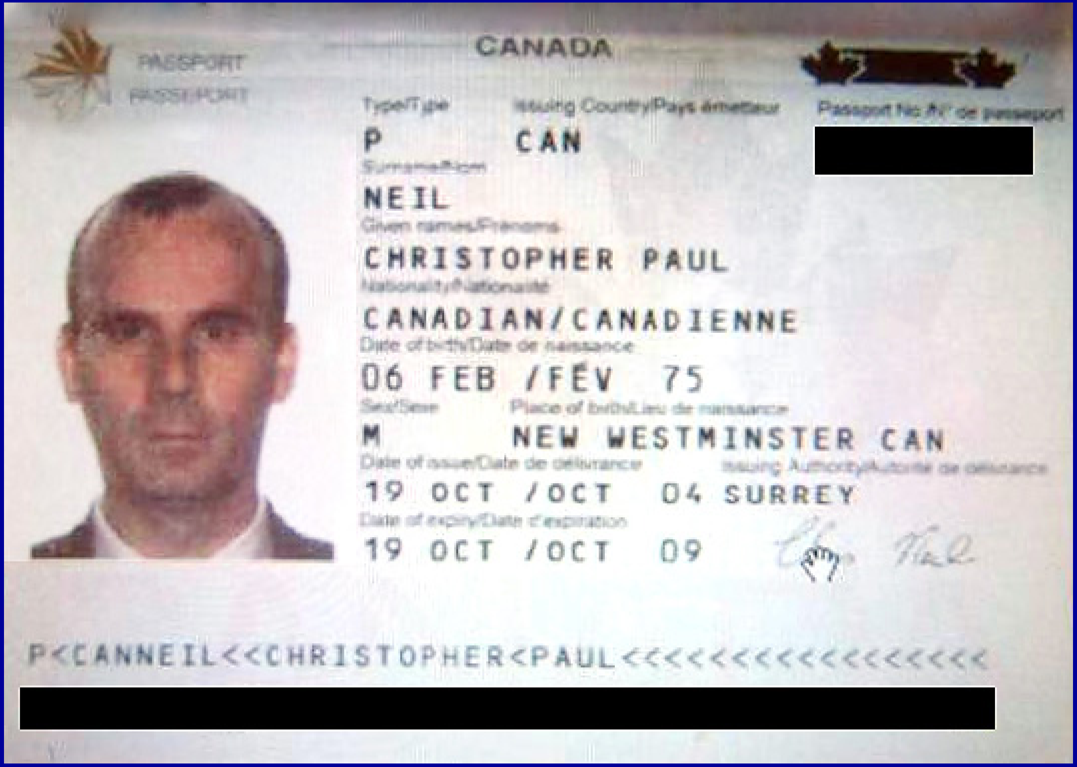
IMMIGRATION
AIRPORT THAILAND

HO 07726

9 NOV 2007

เฉพาะชาวต่างชาติกรุณากรอกข้อมูลทั้งสองด้านของบัตร
For non-Thai resident, Please complete on both sides of this card

Interpol Case: Christopher Paul Neil



PASSPORT
PASSEPORT

CANADA

Type/Type	Issuing Country/Pays émetteur	Passport No/N° de passeport
P	CAN	[redacted]

Surname/Nom
NEIL

Given names/Prénoms
CHRISTOPHER PAUL

Nationality/Nationalité
CANADIAN/CANADIENNE

Date of birth/Date de naissance
06 FEB /FÉV 75

Sex/Sexe	Place of birth/Lieu de naissance
M	NEW WESTMINSTER CAN

Date of issue/Date de délivrance	Issuing Authority/Autorité de délivrance
19 OCT /OCT 04	SURREY

Date of expiry/Date d'expiration
19 OCT /OCT 09

P<CANNEIL<<CHRISTOPHER<PAUL<<<<<<<<<<<<<<<<<

[redacted]

Interpol Case:
Christopher Paul Neil

Host-based Evidence

- Property Intrusion
  - Emails
  - Server Logs
  - Documents
  - Transaction History
  - Spreadsheets
  - Scanned Documents
  - Backup Files

Network-based Evidence

- Child Exploitation
  - ISP Logs of Subscriber
  - IP Address History
  - Logon/Logoff record
  - Subscriber Information
    - Address
    - Phone
    - Form of Payment
    - Contact Person

Network-based Evidence

- Property/Intrusion
- Log files/router/firewall
- Subscriber information
- User activity
- Network Based Content (email, profiles, tweets),
  - e.g. Facebook, Myspace, Linkedin, Twitter

Preservation

- Child Exploitation
  - Screen Capture software
  - Email preservation from Service Provider
  - Direct to Law Enforcement Computer (P2P)
  - Seizure of digital evidence
  - Obtaining an image (exact copy) of evidence

Preservation

- Property/Intrusion
- Screen capture software
- Preservation letter to ISP
- Direct to LE (P2P)
- Seizure
- Imaging

Preservation

- Whichever option you choose:
  - You must collect data in a forensically sound manner.
  - You must protect the integrity of the data
- Confer with a forensic examiner
- What agencies/services are available to process this data?
- Case management is a priority

Questions?