



*International Cooperation in
Combating Cybercrime
– A Real Life Case Example –*

AF CyberSec

Cote D'Ivoire – Africa - 2008

Joel Michael Schwarz

Computer Crime & Intellectual Property Section

U.S. Department of Justice, Criminal Division

(202) 353-4253

joel.schwarz@usdoj.gov

Anatomy of an Investigation: Kidnapping in South America

- 4:34 P.M. -0500 GMT- It begins....
- You are a Prosecutor for the Dept of Justice – you've been on duty all day
- You receive a call from a representative from the Embassy of Country A, in Washington, D.C. - they need your help
- Elderly woman kidnapped approximately 2 weeks ago - No witnesses
- Husband was given 2 index cards by someone unrelated to the kidnapping
 - First index card – name of a hotmail account, kidnapped@hotmail.com, along with a password and instructions
 - Second index card – another hotmail account, we-have-your-wife@hotmail.com, but with no password
 - Asks for \$250,000.00

4:36 P.M. -0500 GMT

- Country A's law enforcement has been investigating for 2 weeks
- No physical evidence
- Need help with Hotmail – which is based in the US
- Country A contacted Hotmail on its own, but:
 - Hotmail – have consent of account holder?
 - Hotmail - need court order from US Court, to release the personal info.
- Country A now seeking US assistance

4:38 P.M. -0500 GMT

- Your first decision – immediate threat to life and limb?
 - elderly woman, but already missing 2 weeks
 - courts still open – will close in a few hours
- Begin drafting papers
- 6:04 P.M. –0500 GMT - race over to the courthouse in a taxi
- Hand papers to judge and wait in chambers
- 6:18 P.M. -0500 GMT - Judge signs
- 6:19 P.M. -0500 GMT - Clerk of Court office
- 6:36 P.M. -0500 GMT - Taxi back to your office
- Call Hotmail and fax order

6:57 P.M. -0500 GMT

- Wait by the phone for Hotmail
- 7:12 P.M. -0500 GMT – Hotmail calls back
 - Name, address and subs info. – bogus
 - Financial data – none (Hotmail = free)
 - IP addresses
- 7:14 P.M. -0500 GMT
 - Provide information to Country A's authorities
- 7:58 P.M. -0500 GMT – Country A finishes contacting providers
 - all IP addresses trace back to cyber-cafes

8:00 P.M. -0500 GMT

- Call from Country A
 - Drive bys of address = abandoned lot
 - Phone = disconnected (registered name = bogus)
 - Name = no hits
- Family received another E-mail
 - attached picture of victim – she's going down hill very fast (looks sick and is missing her meds)
- Only hope is to apprehend while online (to provide drop info) – in cyber café'

8:18 P.M. -0500 GMT

- Speak with FBI Office in D.C. and explain the need to have an FBI agent assigned ASAP – and what the agent will be expected to do
- 8:20 P.M. -0500 GMT - Contact Hotmail (set up pen/trap and link to cell/beeper)
- 8:24 P.M. -0500 GMT – Contact FBI Office in CA – agent assigned
- 8:28 P.M. -0500 GMT – Hotmail activates P/T – automatically copied to agent's cell phone

7:50 A.M. -0500 GMT – Next Morning

- FBI Agent's cell phone goes off – hotmail account accessed
- Agent logs in, runs check on the IP address indicated
- 7:51:35 A.M. –0500 GMT – Agent calls you and you conference in Country A's authorities
- 7:52:42 A.M. – 0500 GMT– Country A's authorities ascertain local address using trace on the IP address (real-time)
- 7:53:00 A.M. –0500 GMT - police car nearest the cyber café' is dispatched
- 7:54:22 A.M. – 0500 GMT – Cyber café' surrounded – kidnapper apprehended while on café' computer
- 7:58 A.M. –0500 GMT – using information provided by suspect, police raid nearby house and recover woman
- 8:00 A.M. –0500 GMT – remaining kidnappers placed under arrest – elderly woman taken to hospital

1st kidnap victim recovered alive, in years

Only accomplished through:

- ability of public safety officials being able to investigate and track in real-time
- ability of public safety officials to cooperate in hours, not days, weeks or months – the speed of traditional international cooperative mechanisms
- and information controller (in this case ISP) being able to disclose information and cooperate with LE in an expedient manner

Lawyer-like disclaimer . . .

- FIN-



Joel Schwarz
joel.schwarz@usdoj.gov
202-353-4253



WWW.CYBERCRIME.GOV

Computer Crime and Intellectual Property Section (CCIPS)
of the Criminal Division of the U.S. Department of Justice