Competencies and Functioning in Practice of the 24/7 Points of Contact

U.S. DEPARTMENT OF JUSTICE

The Crime

- Threat to blow up airport, railway station, and schools
- Letter to Presidential Office: "I'm going to kill your children"
- Simulated bomb discovered near rail line and school

- Country A launches HUGE investigation

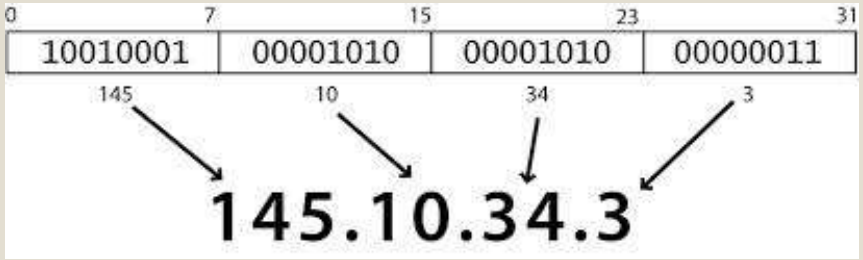
The Crime

- Demands $100,000,000 via a gmail account

Police set up a payment with bag of fake money; suspect does not appear

Stage 1: Request Emergency Assistance from Google

- Country A asks Google directly for the IP address that was used to log into the gmail account.



Result: Google discloses IP addresses directly to Country A law enforcement

… but the suspect is using open wifi

Practical suggestions

- Consider establishing relationship with provider outside of an actual case

Stage 2: Preservation (Day 1)

- Country A calls 24/7 contact for U.S. and asks for preservation of all account data
- Result: U.S. issues data preservation order to Google (90 days)

Practical Suggestions

- Preservation important because of lack of U.S. Data Retention laws (and the speed of foreign assistance)
- Providers may act on preservation requests from foreign law enforcement agencies
- Not all ISPs will keep investigation confidential

Stage 3: 24/7 Request for Content Disclosure

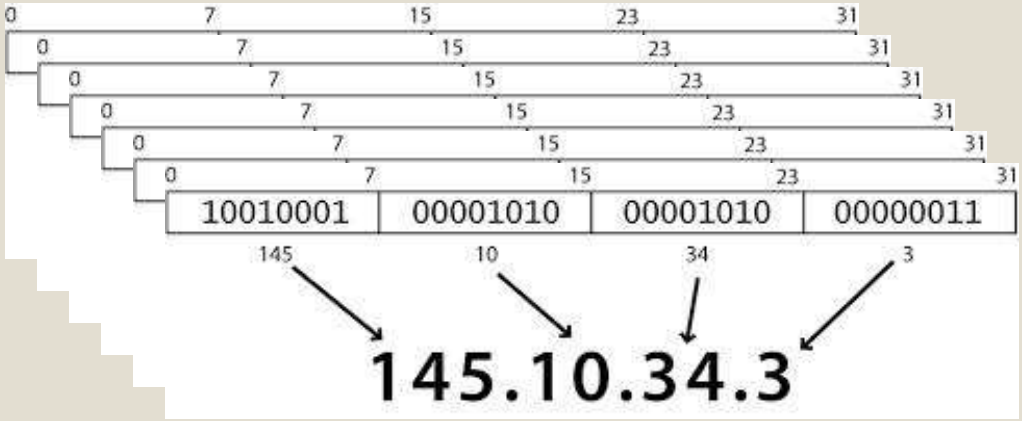
- Through 24/7 contact, Country A asks for the disclosure of the content in the account

Result: Google discloses content to U.S. Department of Justice, who passes content to Country A law enforcement

… but it isn't helpful

Stage 4: Prospective Traffic Data (Day 4)

- Country A makes Mutual Legal Assistance Request (MLAT) that asks U.S. to initiate the collection of traffic data on an ongoing basis



Result: U.S. obtains a court order to compel Google to provide traffic data, which is passed to Country A

… but it is still not enough

Some Practical Suggestions

- Each assertion in an MLAT needs to be supported
  - Not that we don't trust the requester – it is what U.S. law requires
- Common problems:
  - Insufficient factual basis
  - Insufficient support for particular facts
  - Example: "Based on our investigation, members of the criminal group use the following Yahoo! email accounts in their criminal activities."
- Freedom of speech under the U.S. Constitution

Stage 5: MAC address (Day 10)

- Country A discovers the MAC Address of the subject and requests (via MLAT) that Apple disclose whatever information it has

Result

- Apple has name and address of user who registered MacBook Air and 3 iPhones (with phone numbers)

Justice Is Served

- Country A uses lead and conducts a “traditional” investigation; suspect confesses
- Sentenced to 7 ½ years in prison