Investigating Cybercrime:
A Lesson Learns from IWT Online Cases in Indonesia
(2011-2014)

Dwi N. Adhiasto

The Scale of Online Wildlife Trade

Wildlife trade is any sale or exchange of wild animal and plant resources by people that involve live animals and plants or a diverse range of products needed or prized by humans (TRAFFIC, 2008). The value of illegal, unreported and unregulated fisheries alone has been estimated as between USD 10-23 billion per year (MRAG & FERR, 2008), while the value of the illegal international timber trade has been estimated as USD 7 billion per year, and the illegal wildlife trade, excluding timber and fisheries as USD 7.8 – 10 billion per year (GFI, 2011).

The scale of illegal wildlife crime through online trade is also devastating. IFAW's (International Fund for Animal Welfare) report titled Wanted-Dead or Alive-Exposing Online Wildlife Trade (2014), revealed that 33,006 live wild animals and their parts and products were available for sale on 280 online marketplaces (open source website) in 16 different countries in only six week in early 2014. IFAW's investigation also found 9,482 advertisements of CITES (Convention on International Trade in Endangered Species) Appendix II and Appendix I species, conservatively estimated to be worth almost 11 million USD. The Environment Intelligence Agency (EIA) surveyed a Google Japan Shopping site from February 4-22, 2013 and found approximately 1,400 advertisements offering whale products for sale and around 10,000 advertisements offering ivory products for sale.

Online Wildlife Trade in Indonesia

Between 2011 – 2014, the Indonesian authorities handled a total of 34 online cases related to the illegal trade of protected tigers, sun bears, elephants, leopards, gibbons, or birds. The suspects illegally traded wildlife products and live animals through social media, BlackBerry Messenger (BBM), Short Messaging Service (SMS), WhatsApp, and online store communities. The number of online cases has increased since 2011 as a change of strategy from conventional transactions to avoid detection by the police. Conventional transactions (buyer and seller meet in person in the open market or in the black market) were often easy to detect by the police posing as potential buyers. The increased market demand for mobile phones also supports the online trade in Indonesia. AC Nielsen's Global Survey of E-Commerce (2014) reported the ownership of mobile phones increased three times while landline ownership has dropped 50% between 2005 – 2010. Mobile phones and computers are devices most frequently used by Indonesians for online shopping; 61% people use mobile phone and 58% computer. The Indonesian Minister of Communication and Information (MCI) stated that Indonesia has the 4th largest number of Facebook users in the world. According to E-Marketer's report, Indonesia has 83.7 million Internet users in 2014, placing

Indonesia as the 8th largest internet user in the world. Therefore, there is a huge potential market in Indonesia for online trade, including online trade of illegal wildlife.

Regulations

Selling and buying protected wildlife and their parts are prohibited under Article 21 Section (2a), and Section (2d) Indonesian Act No. 5 year 1999 (Conservation of Biological Resources and their Ecosystem). Article 21 Section (2a) states, "Any and all persons are prohibited to catch, injure, kill, keep, posses, care for, transport, or trade a protected animal in live condition". Furthermore, Article 21 Section (2d) states, " Any and all persons are prohibited to trade, keep or possess skin, bodies, or other parts of a protected animal, or goods made of parts of the animal, or transfer from one place in Indonesia to another, within or outside Indonesia". The offenders who violate Article 21 Section (2a) or Section (2d) shall be sentenced to imprisonment for a maximum of 5 years in prison and a fine not exceeding USD 10,000.

The Indonesian Act No. 11 year 2008 is focuses on Electronic Information and Transaction. Based on elucidation of Article 2, "This Law shall apply to any Person who commits legal acts as governed by this Law, both within jurisdiction of Indonesia and outside jurisdiction of Indonesia, having legal effect within jurisdiction of Indonesia and/or outside jurisdiction of Indonesia and detrimental to the interest of Indonesia". Article 30 Section (1) clearly stated a prohibition of "Any Person who knowingly and without authority or unlawfully accesses Computers and/or Electronic Systems of other Persons in any manner whatsoever". Furthermore, in Article 30 Section (3) stated the prohibition for "Any Person who knowingly and without authority or unlawfully accesses Computers and/or Electronic Systems in any manner whatsoever by breaching, hacking into trespassing into, or breaking through security systems". Article 46 Section (1) states, "Any Person who satisfies the elements as intended by Article 30 Section (1) shall be sentenced to imprisonment not exceeding 6 (six) years and/or fine not exceeding USD 60,000". For any persons who violate Article 30 Section (3) shall be sentenced to imprisonment not exceeding 8 years and/or a fine not exceeding USD 80,000.

Indonesian regulations allow electronic interception and wire-tapping for law enforcement and national security purposes. Article 31 Section (3) states, "Interception excepted from one as intended by section (1) and section (2) shall be interception carried out in the scope of law enforcement at the request of the police, prosecutor's office, and/or other law enforcement institution as stated by laws". The interception by law enforcement is important as cited in Article 5 Section (1), "Electronic Information and/or Electronic Records and/or the printouts thereof shall be lawful means of proof". Therefore, the Indonesian police and Civil Service Investigators, conduct joint operations that include digital forensic works to combat illicit online wildlife trade

The Stages in Combating Online Wildlife Trade

A. Desk research

The authorities use Internet browsers such as Firefox and Internet Explorer and search engines e.g. Google to find online wildlife traders. Most traders use popular Electronic Commerce (e-commerce) websites or social network including indonetwotk.co.id, www.kaskus.co.id or Facebook. From 34 online cases investigated by the authorities, 9 cases were found through Facebook, 7 cases through BlackBerry Messenger (BBM), 10 cases from

e-commerce websites, and 8 cases through a combination of Facebook and BBM. Traders offer protected wildlife or wildlife products with photos, and mobile contact numbers. Intensive communication between an investigator posing as a buyer and a trader is then established through SMS, BBM, WhatsApp, or email. During this communication, traders will provide detailed information on the wildlife and then prompts the buyer to transfer a down payment.

B. Defining target

Intensive communication between the authority and a target is crucial to ensure and verify that the live wildlife or wildlife product meets the expectation. At least 25% of animal products such as ivory, tiger bones, or rhino horns being sold in the online market are fake or originate from a different species from the one promoted. Sometimes, the mobile phone numbers provided by traders are unreachable or they only provide an email address. There are also cases where he same trader uses more than 1 account to promote the same wildlife, therefore the verification step is beneficial to verify the trader's identity and define potential traders to be followed up. To date, the traders use a third-party bank account to transfer funds from buyers. Using third party will create a secure layer for buyer and trader because there is no direct money transfer from buyer to trader. Therefore, the authority must identify the third-party to proof an illegal transaction between buyer and trader.

C. Interception

The authority intercepts communication in restricted wildlife trader groups to identify potential traders, copy their data and information, understand their strategy to avoid authority detection, and analyze their response on law enforcement efforts by the authority. The first step is building trust or relationship with the target. The second step is when the trader is willing to chat with the officer (sometime poses as a buyer) after trust has been established. The authority could note down the trader's Internet Protocol (IP) address during the chat sessions. The investigator will then start to intercept the trader's email account and password. This action aims to create remote access execution and to enable to password and information copying from the trader's computer. However, some Internet providers install encryption to hide the user's IP address. Interception can also do by hacking a trader's password or asking the password from the trader's group member already under arrest by the authority. Shadowing a restricted group of traders is like placing a virtual Source of Information (SoI) who sends the information continuously to the authority without being noticed. Interception is also an important tool to arrest more than one trader by using a group member account to bait another trader. The operation to arrest another trader should be done immediately before another trader or group member realizes that their restricted group has been intercepted.

D. *Sting operation*

The authority will set up a sting operation if the evidence provided by the trader fits with the expectation. The trader usually asks for a 10-30% down payment to guarantee the transaction or to avoid buyers who are not serious about buying. The risk of Internet transaction is the buyer losing money if they happen to come across a fake trader, but the percentage of fake traders is less than 5%. To define the trader's location during the sting operation, the police will define the target's location using a specific device. Knowing the location of the trader is important to ensure the right target brings the animal by himself and not send someone else / a courier.

E. Downloading

The authority download data and information from the suspect's mobile phone after the arrest takes place. This is a crucial time to ask for the password or download mobile phone contents before other traders or restricted group of traders realize that a member of their group has been arrested. The investigator must utilize one or two hours after the arrest to crack the password and download the data and information. To date, digital forensic software can recover cellphone data that was erased by the traffickers. The communication between the suspect already arrested and other traders could be used to bait and arrest the other traders within a day/ before the information of the arrest is leaked.

F. Providing electronic evidence

The suspect's family or e-commerce website often erases the suspect's Facebook account or links to wipe out any other evidence. E-commerce website operators are often weak on monitoring products sold by sellers. Erasing the suspect's link on the website will protect the website from public scrutiny or police investigation. However, the police could order the website operator to recover the suspect's advertisement. A police investigator will copy the Facebook page or website screen to show the communication and photos for evidence. The police must provide the electronic evidence to the prosecutor, which shows the suspect dealing in the illegal trade or carrying out a transaction using the Internet. The electronic evidence will be showed to the prosecutor and judge during legal process and courtroom. The electronic evidence strengthens the indictment in addition to the suspect's confession or information from witnesses. The police must provide three components to process the suspect's legal documents, which include the evidence, witness, and the suspect himself. The indictment will be stronger if the police provide a number of evidence and more than two witnesses in court.

Conclusion

The increasing number of e-commerce and social media transactions of protected wildlife and wildlife products showed that traders see the benefit of using the Internet to boost their business. With 83.7 million Internet users in Indonesia and millions more abroad, e-commerce or social media are cost-efficient ways to promote their products. By using the Internet, the traders are able to conceal their identity and transaction. The trader can also send the wildlife products through cargo expedition, which is a safe way to avoid police monitoring.

Both Internet operators and the authority should work closely to identify illegal traders using e-commerce facilities. Internet operators should coordinate with the police to track a trader's history in selling protected animals and their by-products. Furthermore, Internet operators or telecommunication experts could testify as witnesses in court if needed.

Reference:

Indonesian Act No. 5 year 1990. Conservation of Biological Resources and their Ecosystem

Indonesian Act No. 11 year 2008. Electronic Information and Transaction

TRAFFIC. 2008. TRAFFIC; *The Wildlife Trade Monitoring Network*. Retrieved from http://www.traffic.org/trade/

CITES. 2013. *Convention on International Trade in endangered Species of Wild Fauna and Flora; Appendices I, II, and III*. Switzerland. CITES & UNEP publication.

Shipley, T.G., Bowker, A. 2013. *Investigating Internet Crime: An Introduction to Solving Crimes in Cyberspace.* Syngress

AC Nielsen. 2014. *The Nielsen Global Survey of E-Commer*ce. Retrieved from http://www.nielsen.com/id/en/press-room/2014/indonesian-consumers-flock-online-to-purchase-products-and-services.html

Adhiasto, D.N., Giyanto. 2014. *Perdagangan Online Harimau Sumatera di Indonesia. An abstract for Indonesia Tiger Conference*. Wildlife Conservation Society-Indonesia Program. Bogor.

E-Marketer. 2014. Top 25 Countries, Ranked by Internet Users. Retrieved from www.emarketer.com

McCrea T., Steele. 2014. *Report: Wanted-Dead or Alibe-Exposing Online Wildlife Trade*. IFAW London.