**Budapest Convention – Case Study**

**Background**

Middle Earth is a small fictious developing country in Africa and a neighbor of two other countries, Rohan and Mordor. It is a member of the WTO, the UN and is a party to the Budapest Convention on Cybercrime. Middle Earth has traditionally been a centre of a thriving banking and finance industry. Its largest bank Middle Earth National Bank (“MENB”) has several branches in the region and internationally. Middle Earthean is the official language of Middle Earth.

You are a law enforcement official of Middle Earth and are responsible for investigating cybercrimes in Middle Earth.

**Part 1 - Substantive Law**

You receive an anonymous report that cybercriminals have hacked into the main server of MENB. The cybercriminals have installed malware which randomly changes the size of the mouse cursor and the background wallpaper of all computers connected with the main server. Your investigation suggests that the malware was created by a group of hackers known as “DarkHacker”.

As part of your investigation, you identify the official website of DarkHacker as www.darkhacker.com. You observe that software ostensibly designed for translating text Middle Earthean language to English is being sold on the website, but the software is marketed as also enabling hacking into computers..

Your investigation also reveals that fingerprint data that enables access to laptops and smartphones is being sold on [www.darkhacker.com](http://www.darkhacker.com). In an attempt to identify the individuals operating DarkHacker, you conduct an undercover operation and purchase fingerprint data from www.darkhacker.com.

**Questions:**

* What cybercrime(s) was committed by hacking into and installing malware on the MENB server?
* What cybercrime(s) can you identify as being committed by DarkHacker?
* Did you commit a cybercrime offence by purchasing fingerprint data from DarkHacker?

**Part 2 – Procedural Law**

As part of the undercover operation to purchase fingerprint data from DarkHacker, you are prompted to enter your email address to receive payment instructions. You receive an email from an email account [criminal@scammail.com](mailto:criminal@scammail.com) with instructions on how to make the payment using Bitcoin.

Your initial investigation reveals that the email service provider for [criminal@scammail.com](mailto:criminal@scammail.com) is Scam Mail Inc. You identify its website as [www.scammailinc.com](http://www.scammailinc.com). You learn from its website Scam Mail Inc has its head office and only data center in Middle Earth. You also learn that Scam Mail Inc. only retains data for a period of 7 days after which all data is deleted.

You consider using the email addresses to identify the individuals behind DarkHacker.

You also consider obtaining details of other people contacted through the email account [criminal@scammail.com](mailto:criminal@scammail.com) in the last seven days.

**Questions:**

* What initial measures should you take to ensure that the investigation process is not frustrated?
* What kind of information would you need to identify the person using [criminal@scammail.com](mailto:criminal@scammail.com)? How can you obtain such information from Scam Mail Inc?
* How would you seek information from Scam Mail Inc regarding other persons contacted by [criminal@scammail.com](mailto:criminal@scammail.com) in the last seven days?

**Part 3 – Other Forms of Cooperation**

Upon making the payment through Bitcoin, you receive another email from an email account fraud@hackmail.com with the fingerprint data attached.

You again consider using the email address to identify the individuals behind DarkHacker. Your initial investigation reveals that Hack Mail Inc (headquarters in Mordor) does not have any office or data centers in Middle Earth but recently published advertisements regarding its free services in Middle Earthean language. Hack Mail Inc stores subscriber information in the form of computer data.

You learn of several persons in Mordor who have complained on different online forums of incidents of fraud allegedly perpetrated by the user of [fraud@hackmail.com](mailto:fraud@hackmail.com). You wish to use these complaints as evidence in subsequent proceedings. Moreover, you contact these persons for information and they are willing to consent to you accessing their email accounts and email messages.

**Questions:**

* What kind of information would you need to identify the person using [fraud@hackmail.com](mailto:fraud@hackmail.com)?
* What is the most expeditious measure to obtain such information from Hack Mail Inc?
* What is the most expeditious way to obtain emails sent by user of [fraud@hackmail.com](mailto:fraud@hackmail.com) to victims in Mordor?

**Part 4 – Mutual Legal Assistance**

Upon analysis of the information you received from Hack Mail Inc. and Scam Mail Inc., you identify one individual part of the DarkHacker group: Boris Smith, a Middle Earth national.

You arrest Boris Smith in Middle Earth and he discloses the location of the computer system being used by DarkHacker in Rohan. As the fact that Boris has been arrested is not public, there appears to be no reason to believe that the data in the DarkHacker computer system is vulnerable to loss or modification.

Smith informs you that the account [fraud@hackmail.com](mailto:fraud@hackmail.com) was used to contact other DarkHacker agents. He also informs you of large scale transaction for the sale of Debit Card PIN codes planned to be undertaken the following day at 17:00 using the same email account.

* What measures can you take to ensure HackMail Inc. preserves data relating to the account [fraud@hackmail.com](mailto:fraud@hackmail.com)?
* What measures should you take to identify other service providers involved transmitting communications related to the DarkHacker scam?
* What measures can you take to obtain computer data from the DarkHacker computer system?
* What measures can you take to ascertain the location of the DarkHacker customer who is planning to purchase Debit Card PIN codes?