**Budapest Convention – Case Study**

**Background**

You are a law enforcement official of Middle Earth, a small fictitious country neighboring two other countries Rohan and Mordor. You are responsible for investigating cybercrimes in Middle Earth.

**Part 1 - Substantive Law**

You receive an information report that data drives of computer systems of a renowned financial institution have been hacked by unknown cybercriminals and malware which increases the size of the mouse cursor has been installed onto those computer systems. Your investigation suggests that the malware was created by a hacking forum called “DarkHacker”.

Further investigation reveals that translation software primarily designed for hacking into computers is also being sold by DarkHacker with the slogan “Buy our translation software & get friends to install it – you can access their computers w/o right!”

In an attempt to identify the individuals operating DarkHacker, you conduct an undercover operation successfully procuring access codes enabling access to computer systems.

**Questions:**

* What cybercrime(s) was committed by installing malware into the computer systems of the renowned financial institution?
* What cybercrime(s) can you identify as being committed by persons on DarkHacker?
* Did you commit a cybercrime offence by procuring access codes to computer systems on DarkHacker?

**Part 2 – Procedural Law**

As part of the undercover operation, you obtain access codes and payment information from a DarkHacker agent. You receive an email from a paid email account [criminal@scammail.com](mailto:criminal@scammail.com) with a download link to the access codes.

Your initial investigation reveals that the email service provider for [criminal@scammail.com](mailto:criminal@scammail.com) is Scam Mail Inc. Scam Mail Inc has its head office and only data center in Middle Earth.

You learn from its website 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 DarkHacker agent.

The information you obtain suggests that the scale of operations is much larger than initially anticipated. You think it is now necessary to obtain information of other unknown 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**

You click on the link to download the access code and receive another email from a free email account fraud@hackmail.com with bank details.

You again consider using the email address to identify the DarkHacker agent. 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 Earth in local language.

Hack Mail Inc stores subscriber information in the form of computer data.

You also separately learn of several persons in Mordor who have complained on different public 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 the person using [fraud@hackmail.com](mailto:fraud@hackmail.com) to the complainants?

**Part 4 – Mutual Legal Assistance**

As a result of analysing the data obtained you identify one individual responsible for selling the data and providing services: 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 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 selling of bank PIN codes planned to be undertaken the following day at 17:00 using the same email account.

* What measures can you take to ensure HackMailInc 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 bank PIN codes?