Kelompok 7:

* Rionel Irawan / 2440009181
* Gabriela Jazeline Celosse / 2440054134
* Ivany Regina Sidabutar / 2440106251

**2019-03-19 - TRAFFIC ANALYSIS EXERCISE - LITTLETIGERS**

LAN segment data:

* LAN segment range:  10.0.90.0/24 (10.0.90.0 through 10.0.90.255)
* Domain:  littletigers.info
* Domain controller:  10.0.90.9 - LittleTigers-DC
* LAN segment gateway:  10.0.90.1
* LAN segment broadcast address:  10.0.90.255

Task :

**Executive summary:**

**On 2019-03-19 at ??:?? UTC, a Windows host used by ????????? was infected with ???????**

**Details of the infected Windows host:**

**IP address:  
MAC address:  
Host name:  
Windows user account name:**

**Indicators of Compromise:**

*[List of URLs, domains, IP addresses, and SHA256 hashes related to the infection should appear in this section]*

Ans :

Filter : Kerberos.CnameString

Text

Description automatically generated

**Host name:** BOBBY-TIGER-PC$ **Windows user account name:** bobby.tiger

Table

Description automatically generated

**IP address:** 10.0.90.215 **MAC address:** 64:32:a8:57:2b:42

Alert file

Graphical user interface, text, application

Description automatically generated

**On 2019-03-19 at ??:?? UTC, a Windows host used by bobby.tiger was infected with Trojan**

Text

Description automatically generated

**On 2019-03-19 at 1:49 UTC, a Windows host used by bobby.tiger was infected with Trojan**

**Indicators of Compromise:**