CCDC Inject

INJECT NAME	Verify Presence of Exfiltrating Malware
INJECT ID	SOCS05A

INJECT DESCRIPTION:

The CSIO has been cautioned that the internal network may be infected with malware that is exfiltrating data as well as beaconing out for CnC functions. Sample an hour's worth of traffic to validate whether this is actually happening within our network or not.

INJECT DELIVERABLE

Respond with a business memo which provides:

1. For an explanation as to how you made your determination. Be specific as to devices, features and tools used.
2. Provide a conclusion as to whether this is a concern or not, and how you determined that conclusion.
3. Provide evidence of your work using screen shots.