**Bilkent University**
**CS479 – Introduction to Cyber Security**
**Assignment – 2**

Go over “Network Analysis” slides one more time, remember our way of analyzing the PCAP file, searching for IOCs and delivering evidences.

Apply the same methodology using tcpdump one more time. Create your own filters, use linux commands (grep, awk etc.) where necessary.

Create a report stating your filters and outcomes.

The report should include the following data at least for each case:

- Respective tcpdump filter and linux commands if used.
- Outcome of the previous step.
- The interpretation of the outcome (e.g. type of attack, name of possible malicious activity)

*Send your report to emre[dot]yuce[at]bilkent[dot]edu[dot]tr*

**DEADLINE: 06.03.2019 23:59**