Ursnif incident report

* Write an incident report based on the pcap files.

The incident report should contain the following sections:

* **Executive Summary**: State in simple, direct terms what happened (when, who, what).
* **Details**: Details of the victim (hostname, IP address, MAC address, User account name,…etc).
* **Indicators of Compromise (IOCs)**: IP addresses, domains, and URLs associated with the infection.  SHA256 hashes if any malware binaries can be extracted from the pcap.
* **Technical description**: Using the indicators of compromise, describe the stages of infection according to the kill-chain model.
* **Impact**: State the possible impact of the infection.
* **Recommendations**: State what should be done in order to prevent in the future any similar infection.