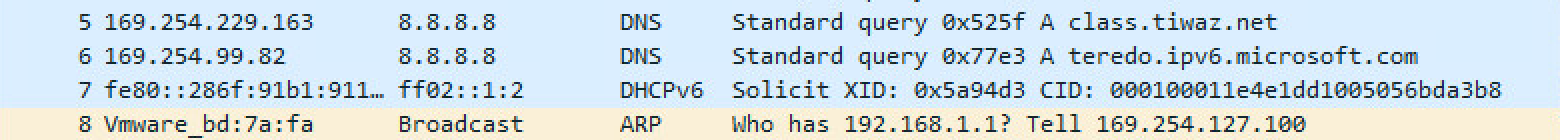
CND Homework 6

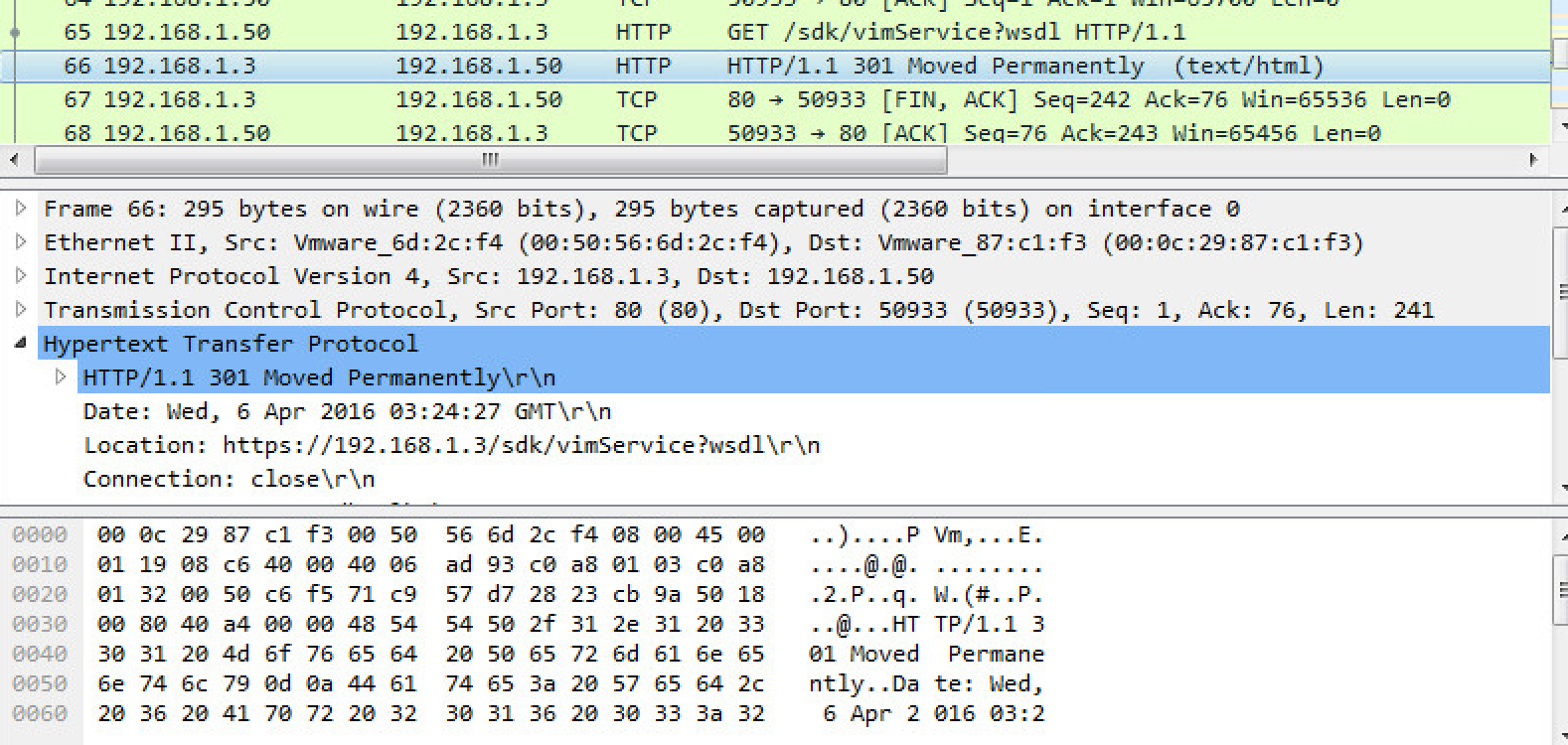
Rajat Vij

Ans 1. Result of analysis on plugin1.exe malware:

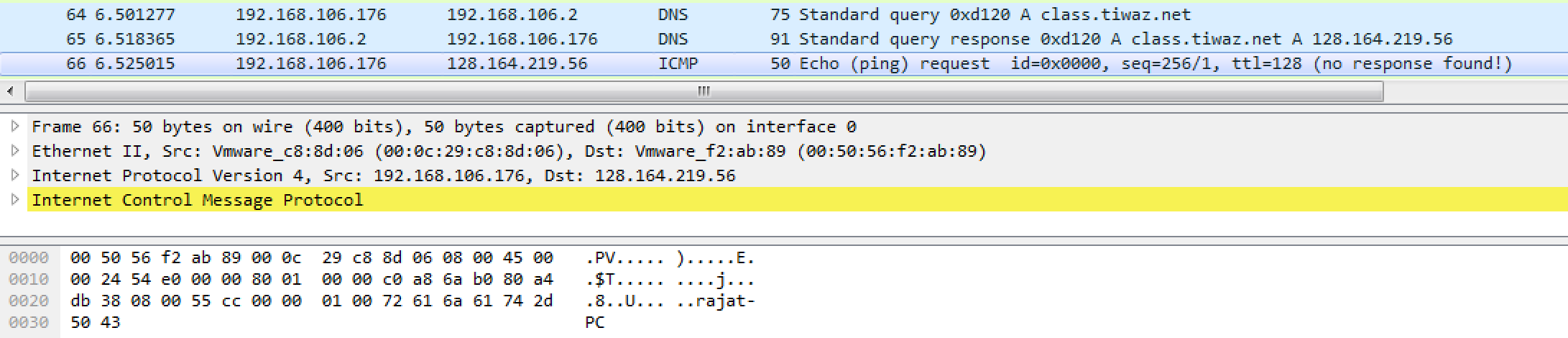
* Using Wireshark on the provided VM where it seems the box is not connected to class.tiwaz.net, I can see the exchange of HTTP packets between our host and 192.168.1.3. We are also also able to observe DNS requests to toredo.microsoft.ipv6 which indicates that their might be tunneling involved in network.

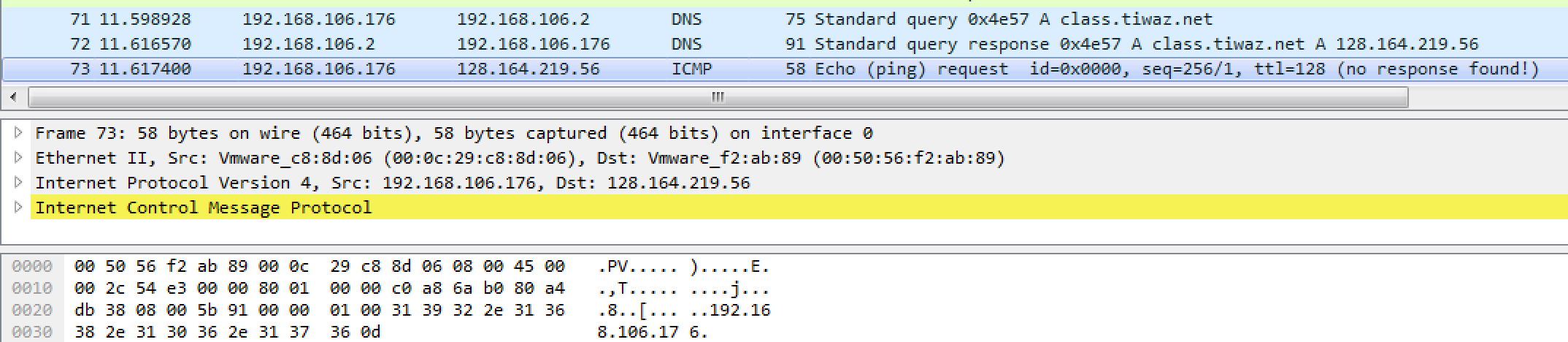


../../Screen%20Shot%202016-04-06%20at%201.47.01%20PM.png



* Using Wireshark on a VM which is connected to the internet and is able to connect to class.tiwaz.net, I are able to see the our host is sending hostname and ip address repeatedly to class.tiwaz.net(128.164.219.56) using ICMP ping.



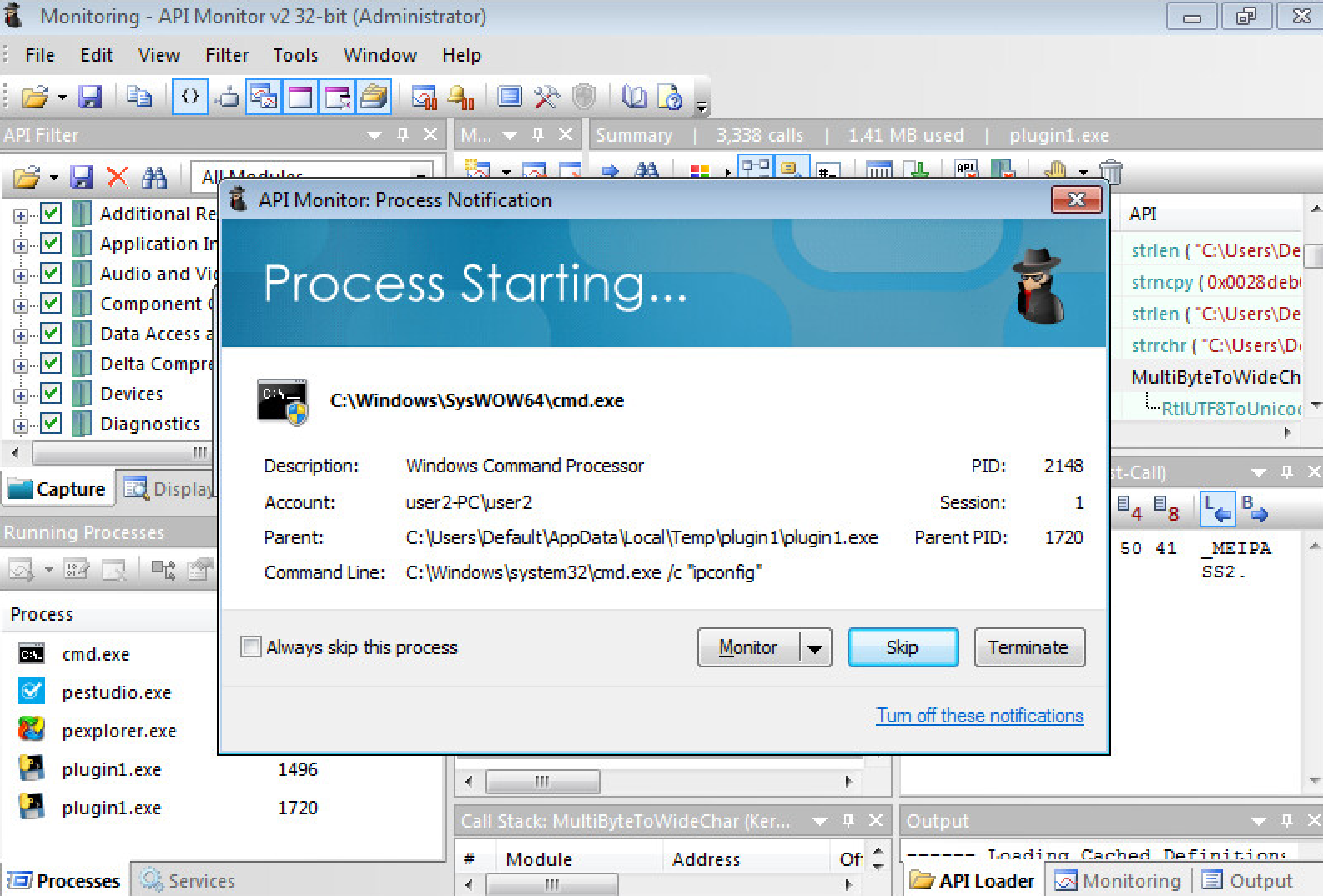


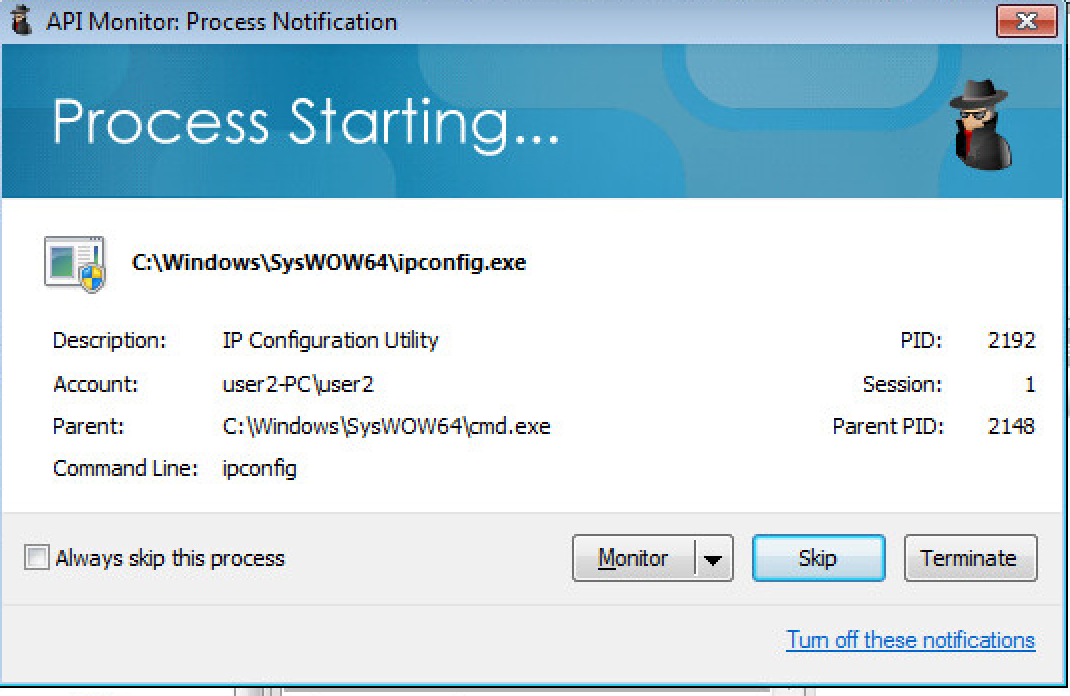
Created a Python Stix Script to generate xml for the target ip address.

* Using Wireshark on both VM’s I noticed the list of ip address which are involved in TCP Packet exchange, I can also observe NBNS packets for the provided VM.

Created a Python Stix Script to generate xml for the list of ip addresses.

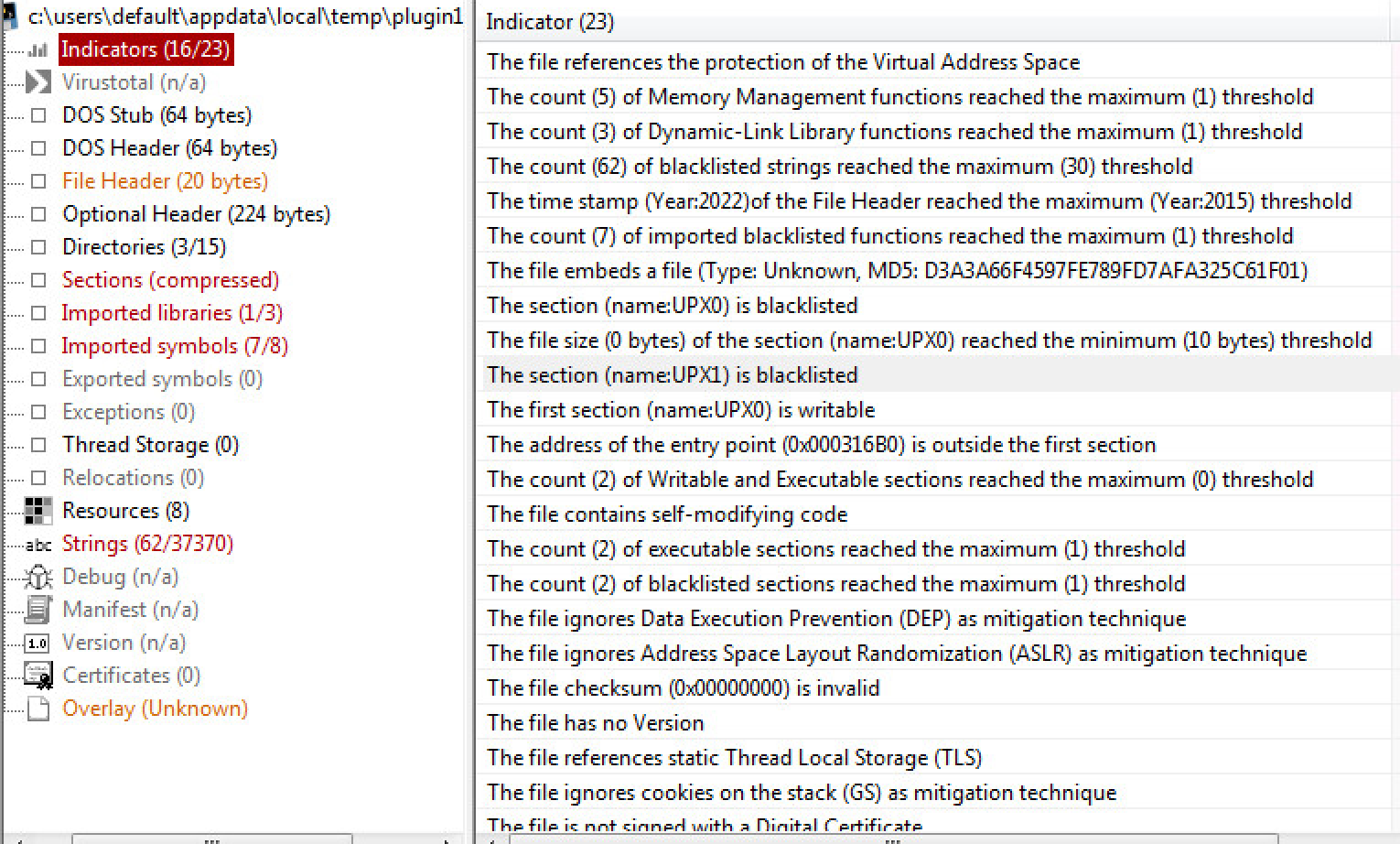
* Using API monitor I learned that this malware is accessing a commandline to get ip address and hostname using ipconfig.





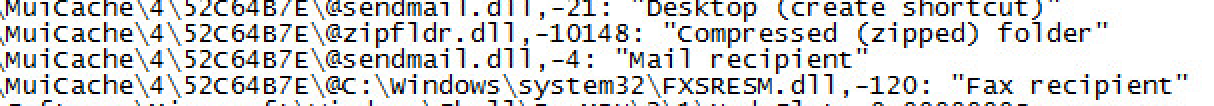
Tried to created a Python Stix script to generate xml for the observed behavior, but was a little confused what to put there. It seemed more like an incident than an indicator.

* Using PE Studio I found that this malware is generating another file of unknown type and embedding that with an suspicious MD5 Hash.
* Timestamp is of a future date.
* File is a self-modifying code, uses python27dll and blacklisted windows socket library for that.
* Has invalid checksum and digital certificate.

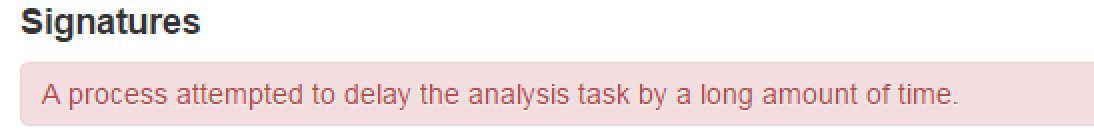


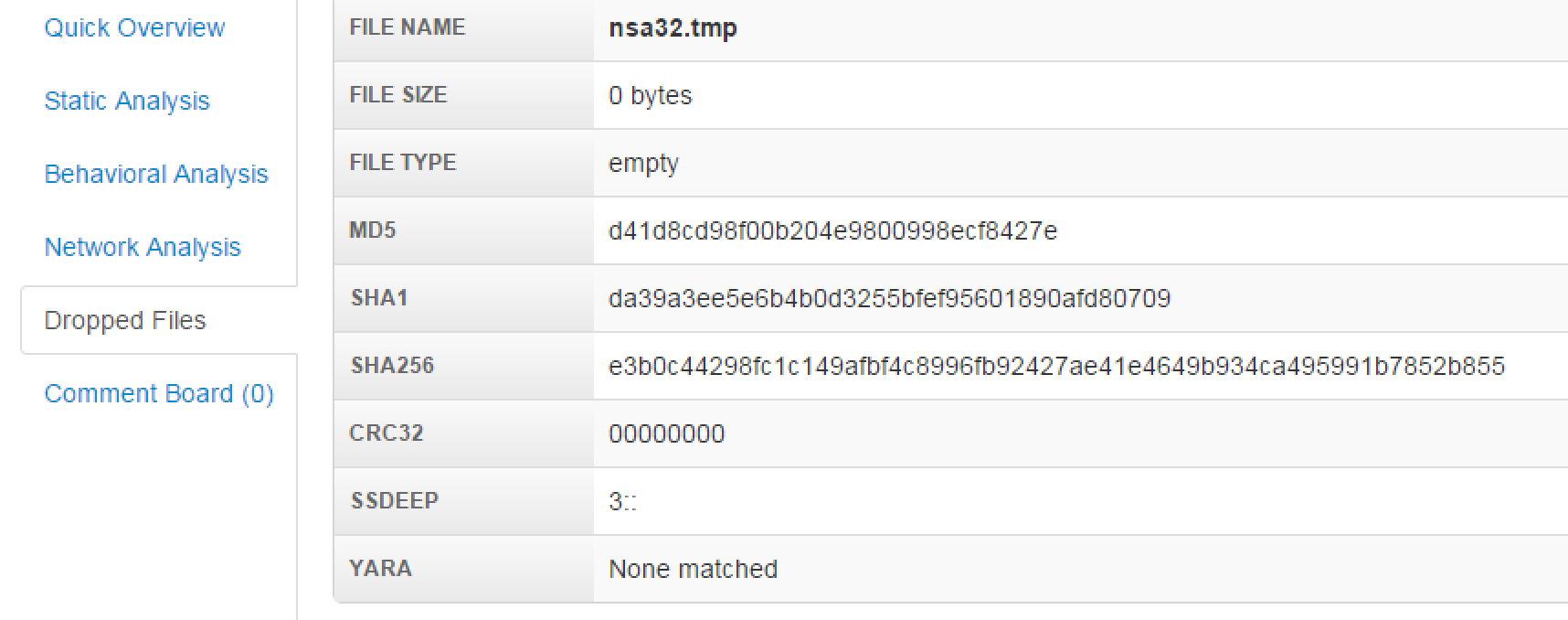
Created a Python Stix script to generate xml for suspicious MD5 Hash.

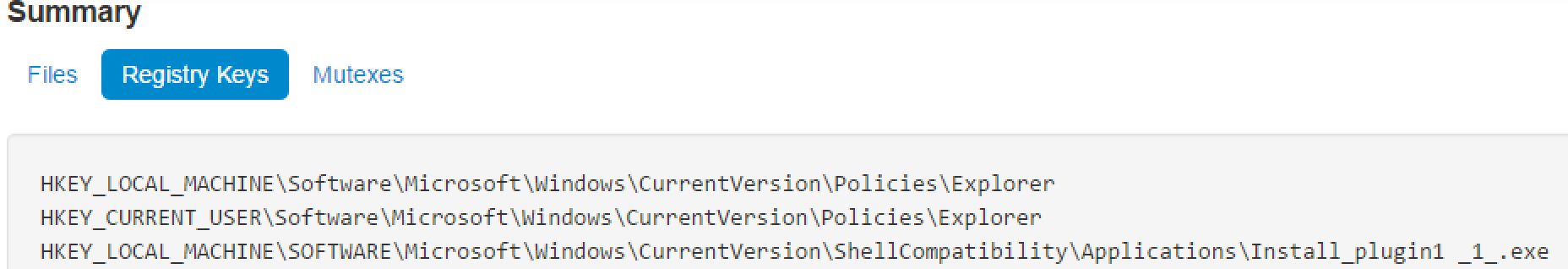
* Using Regshot we are able to identify that the malware is changing or adding registry keys and values targetting Explorer/Userassist and Explorer/MountDevices. It is also targeting services of Mailer and Fax and Scanner.

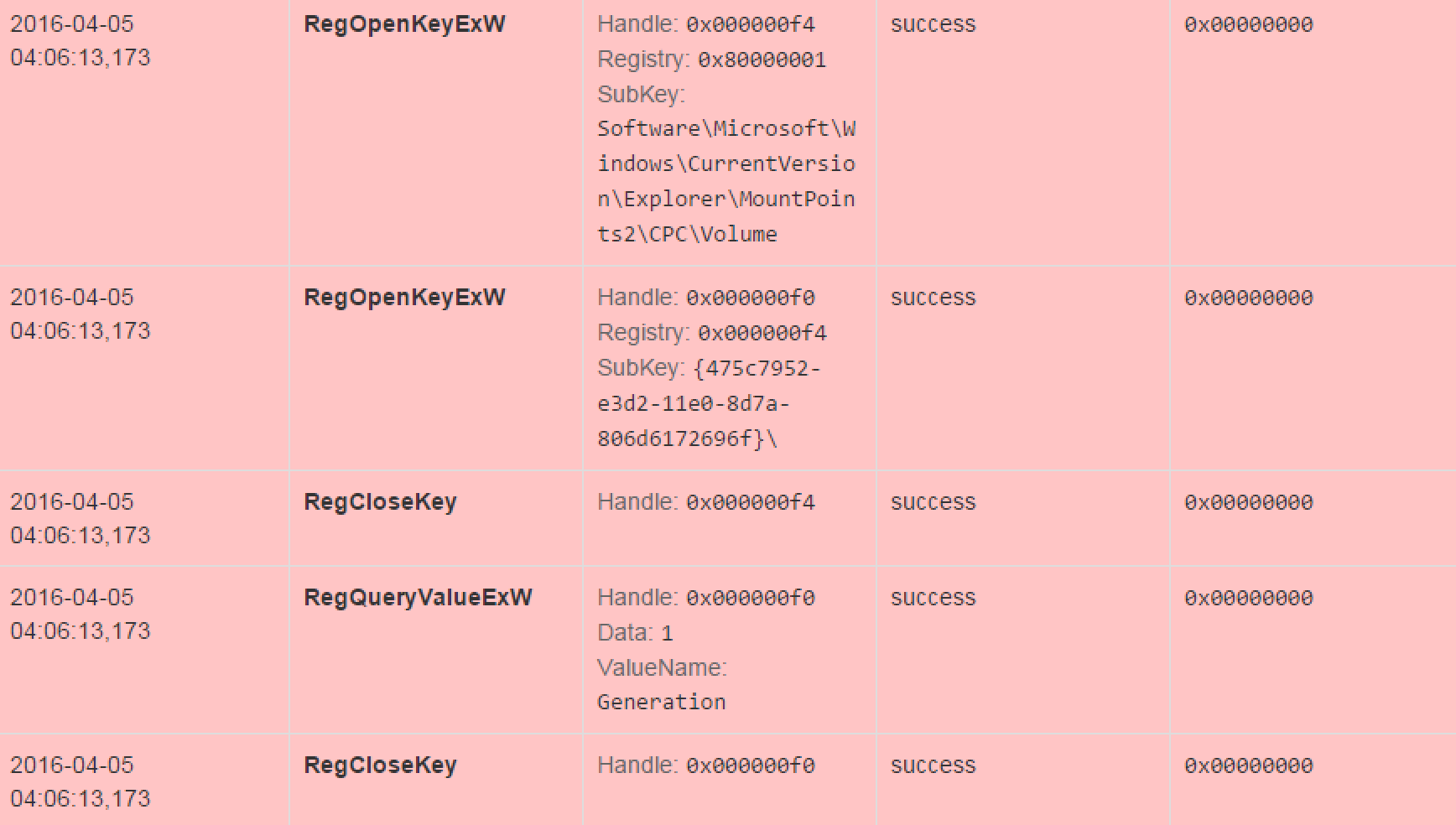


* Using analysis on malwr.com site I can identify that malware is successfully modifying reg key values for Explorer/MountDevices, Explorer/Advanced, Explorer/Policies.
* It is also creating nsa32.tmp in temp folder and msctfime.ime in system32 folder which might contain keylogging info.
* It is also trying to change Default font to Tahoma.
* It is trying to get the information on list of mounted devices.
* It also has signature that tries to delay its analysis in a sandbox environment as a mitigation technique to identify itself.
* It repeatedly writes data to REGDBVersion value for COM3 Registry and enables COM.









Created a Python Stix script to generate xml for affected assets.

Ans 2. For this I parse the most recent list of TOR exit nodes from the link given in the last page of slides and dynamically creates a python file to generate xml for incident/ttp for most current list of tor exit nodes using a python script.