**Malware Traffic Analysis using Wireshark**

Malware traffic or Malicious traffic (malicious network traffic) is any suspicious link, file or connection which is sent through network in order to compromise the target system by an attacker. Malware traffic is a threat that creates the risk which can be impactful for the organization's security or victim’s personal computer.

Wireshark Packet Analysis tool

Free and open source protocol analyzer that can record and display packet captures (pcaps) of network traffic.

Download Wireshark from following link

<https://www.wireshark.org/download.html>

Task:

Download the pcap file from courseweb and open it in Wireshark tool for packet analyzing.

Answer the following questions.

1. What is the date and time of this activity?
   * 2014-11-16 02:11:49
2. What is the IP address of the Windows host that gets infected?
   * 172.16.165.165
3. What is the MAC address of the infected Windows host?
   * 00:50:56:f3:ca:52
4. What is the host name of the infected Windows host?
   * K34EN6W3N-PC (Used DHCP requests)
5. What is the domain name of the compromised web site?
   * www.ciniholland.nl
6. What is the IP address of the compromised web site?
   * 82.150.140.30 (http.request.method == GET)
7. What is the domain name that delivered the exploit kit (EK) and malware payload?
   * stand.trustandprobaterealty.com
8. What is the IP address that delivered the EK and malware payload?
   * 37.200.69.143
9. What is the redirect URL that points to the EK landing page?
   * http://24corp-shop.com/
10. What browser was used by the infected Windows host?
    * Mozilla/4.0 (Follow TCP stream – User Agent)