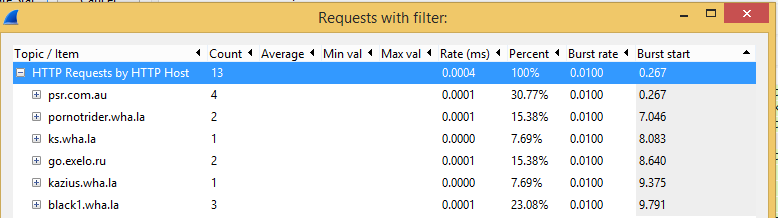
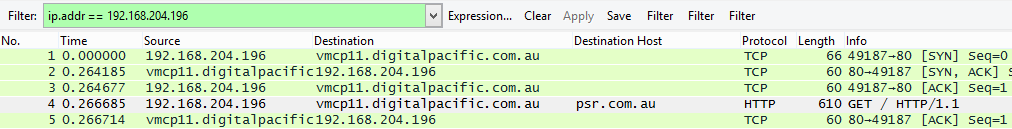
In this pcap file, the host that was infected is 192.168.204.196.

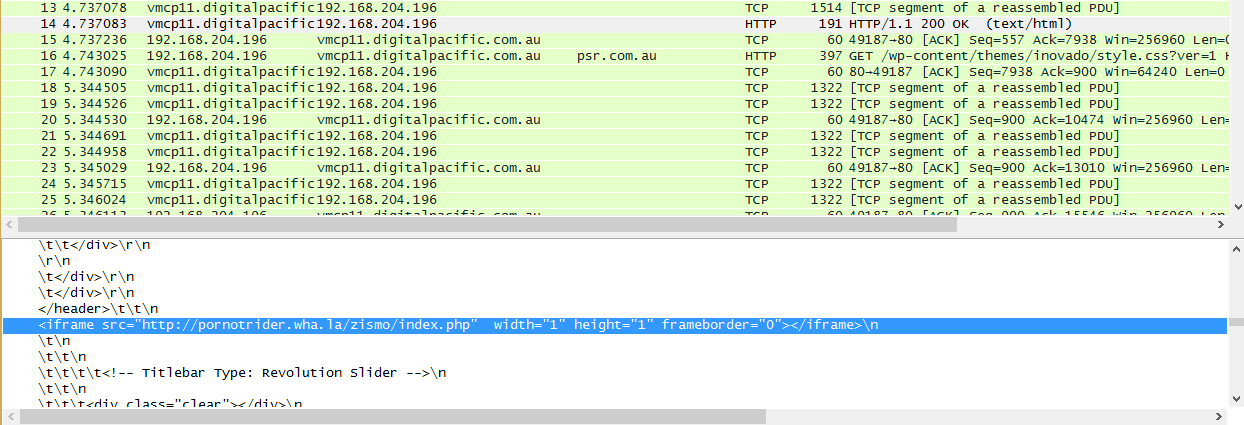


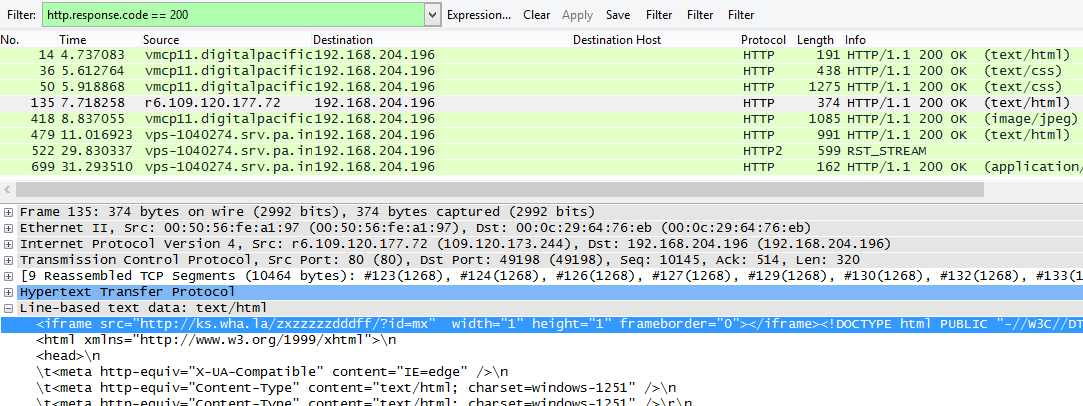
Firstly, I create a HTTP Reqiests in Wireshark and we will see a nice simple view of the order in which everything happened. As we see, after the victim visited the compromised site, psr.com.au, it was redirected to four additional different websites before being sent to the malicious server hosting the blackhole exploit kit. During the following analysis, we will see how the host was redirected to these servers.

In frame 4, we will see the host wanted to visit the destination, vmcp11.digitalpacific.com.au but it was redirected to the destination host which was psr.com.au. Using other words, the psr.com.au domain was using vmcp11.digitalpacific.com.au as their web hosting provider.

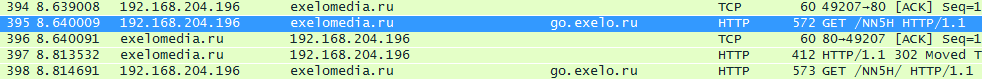


Then, we will see a series of GET requests from the victim browser to psr.com.au. In frame 14, there is an info, "HTTP/1.1 200 OK" which is means the GET request download from the server, psr.com.au was successful. When I click the Line-based text data, we will find there is an iframe and psr.com.au cause the first redirect to a server at destination host pornotrider.wha.la.

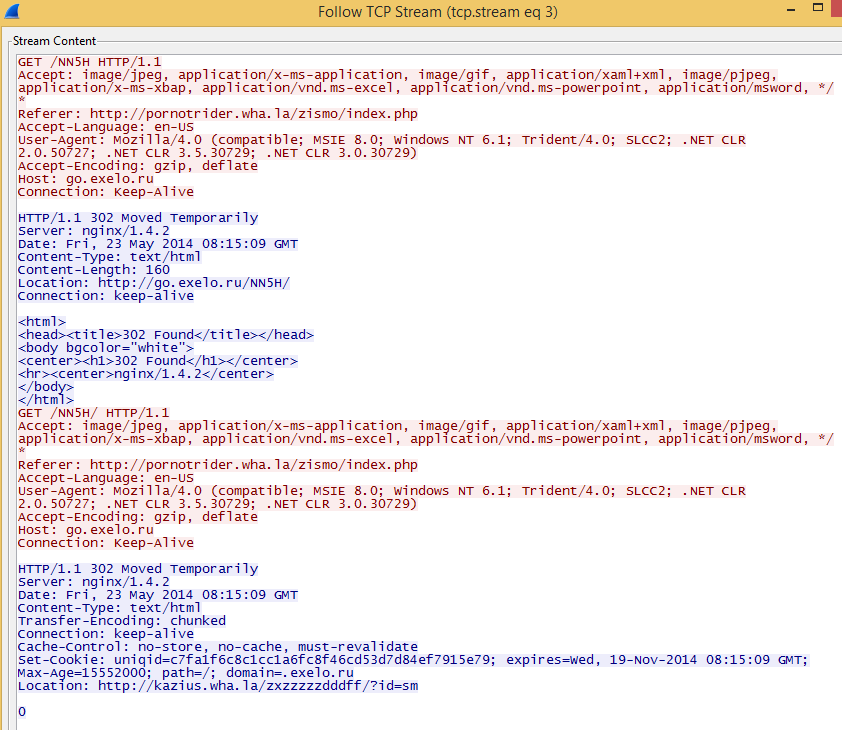
In frame 135, there is a same info, "HTTP/1.1 200 OK". When I click the Line-based text data, we will find there is an iframe too and the pornotrider.wha.la server caused a second redirect to the ks.wha.la server.



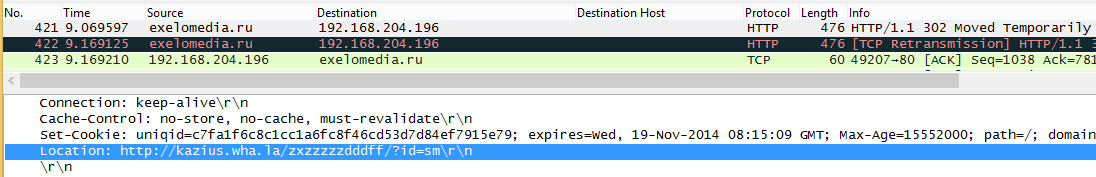
In frame 395 and frame 398, the ks.wha.la server caused a redirect to occur to go.exelo.ru.



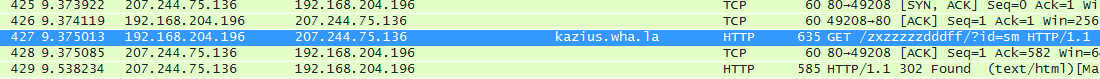
Then, I open these two frame’s Follow TCP Stream and we will see a traditional redirect. The referrer is http: //pornotrider.wha.la and wha.la/zismo/index.php and the location is go.exelo.ru.



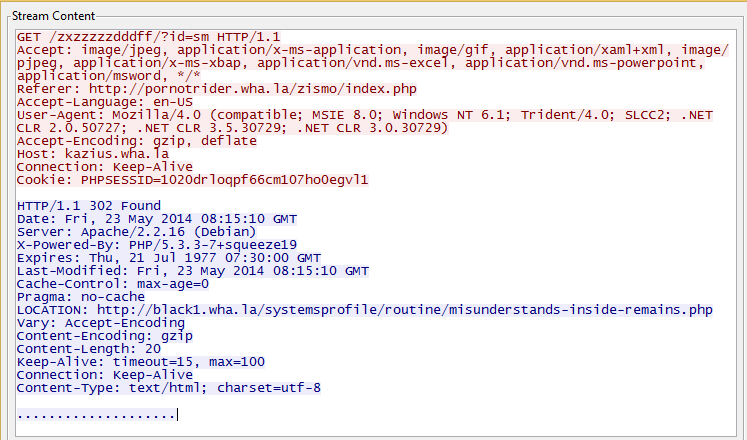
In frame 421 and 422, another redirect to karzius.wha.la occurred after the victim visited the exelomedia.ru server.



In frame 427, the karzius.wha.la server caused the victim to be redirected to the actual blackhole exploit kit landing page.



After opening the frame’s Follow TCP Stream, we will see the victim’s receiving location is <http://black1.wha.la> which is the actual blackhole exploit kit landing page.



In frame 499 a browser exploit was delivered. Follow the TCP stream, we know its exploit has java and the payload has Zues. I think it is blackhole exploit kit.



Lastly, a malicious executable was downloaded by the host from the blackhole server.  As we see, it happened in frame 780. After I open this frame’s Follow TCP Stream, we will see there is an exe file has a header of “MZ” and states “This program cannot be run in DOS mode.”

