Drive by download: you go to a website and you don’t necessarily click on anything or interact with any of the links. The web browser initiates the download immediately.

Anything that starts with 3 is a redirect. HTTP status code is 301 for response (askmen.com). 301 does not render anything. You can see this by following HTTP Stream and you will see there isn’t any data that is encoded. It is only the location that matters for a 301. You can see status codes by inspector tools > network on browser. The first request will redirect the user to www.askmen.com. The second GET request will request to be redirected to www.askmen.com (don’include the /r/n because that is a newline character. Every thing will have this...go look in wireshark).The response code for the second GET request is 200 (successful) meaning that content was fetched from the web server and rendered on the client’s web browser.

You can look at the data encoded in utf-8 (ASCII) and determine what is wrong with the code. You can not always download the HTML code and double click to see what the web page rendered because a lot of times the content may not exist anymore and the web page has changed. Therefore, you want to analyze the html code. Now, the real question is what do you look for when looking at this data? Look at JS, Scripts, CSS, EXE, Flash file, JAR file (java applet when loaded in browser), and PDF. Especially when the JS is running scripts.

MZ is in the data encoding (when you follow HTTP stream) denotes an extension (EXE file). Instead of following and closing HTTP stream for every packet, you can just go to file > export objects > and save all to a directory. After you do that, you can open with text editor and inspect with a lot less headache. HINT: d2.php is the start of the malware. I need to find how to get there. (Also check out pdf and jar later after finding link). I can also deobufuscate code using that language’s parser. For example, if I am dealing with JS, google online JS parser and execute it on there (BEWARE in real life because this can infect your system...you want to do this on a VM).