Detecting Mobile Malicious Webpages in Real Time

Mobile specific webpages differ significantly from their desktop counterparts in content, layout and functionality. Accordingly, existing techniques to detect malicious websites are unlikely to work for such webpages. In this paper, author implements kAYO, a mechanism that distinguishes between malicious and benign mobile webpages. KAYO makes this determination based on static features of a webpage ranging from the number of iframes to the presence of known fraudulent phone numbers.

Now-a-days separate web pages are designing for mobile devices and to steal data from user mobile some malicious web designer will put links in the website, when user click on such link then user will be directed to malicious page which will steal user information from device. To overcome from such issues many application has design but they were not evaluating all features to detect malicious pages compare to this paper technique KAYO.

In KAYO author is using below features to detect weather web page is malicious or benign

1. Mobile specific features : using this feature we will check weather website is making call or sending sms from user mobile by using mobile api called tel:, sms:, smsto:, mms: and mmsto. This feature will further check weather receiver call phone no or receiver sms phone no is in malicious phone directory, if it’s from malicious directory then will consider page as malicious. (Here we are checking only weather web page contains mobile api call more than 3 then will consider as malicious web page and we are not checking malicious phone no as this feature can be use in real time application.
2. JavaScript features: in malicious web pages malicious web designer will use more no of noscript tags, using external java scripts tags (which refer to javascript running on other server) and will use more no of java scripts tags. If any web pages contains noscript tags, external java script and java script tags greater than given threshold then that page consider as malicious otherwise consider as benign.
3. HTML features: In this feature we will check weather link contains more no of domains or not. If link contains more domains then that page consider as malicious. For example in below link we can see more domain such as mobile/web/m/

http://xyz.com/mobile/mobile/web/m/mobie?m=1, /mobil, /m home

the above link will consider as malicious

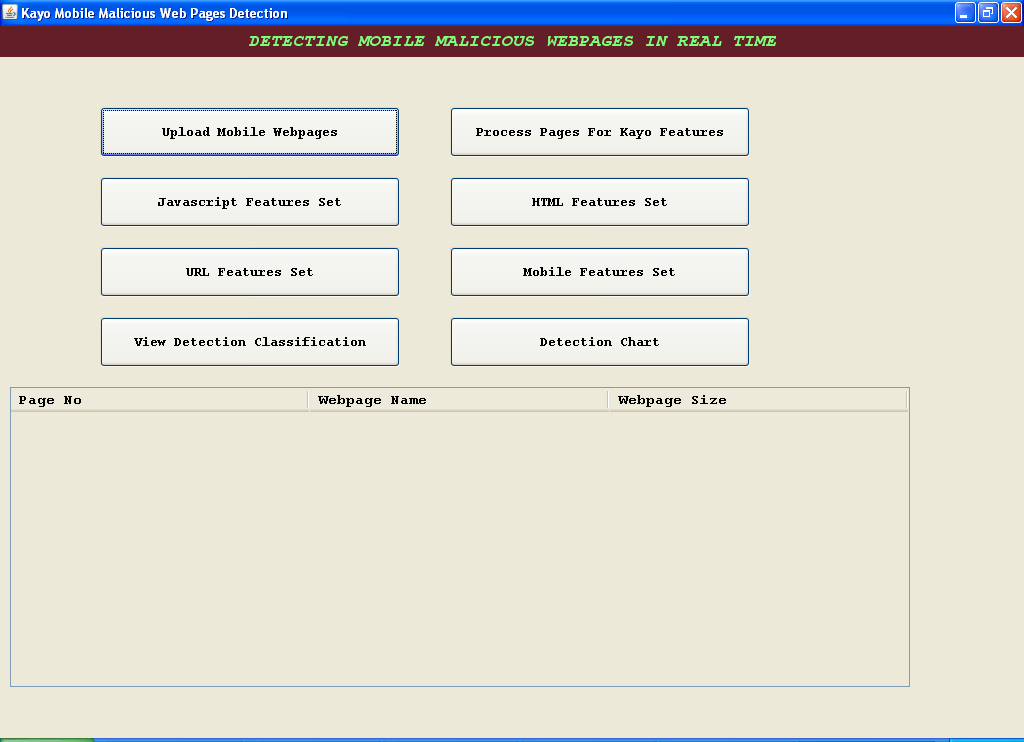
1. URL features: Malicious web page designer will use keywords such as login and bank in the links to mislead users or to make user to visit that page. In this feature also will check if any webpage contains bank and login keywords greater than threshold then that page consider as malicious

In this paper author is using above features to identify web page is malicious or not.

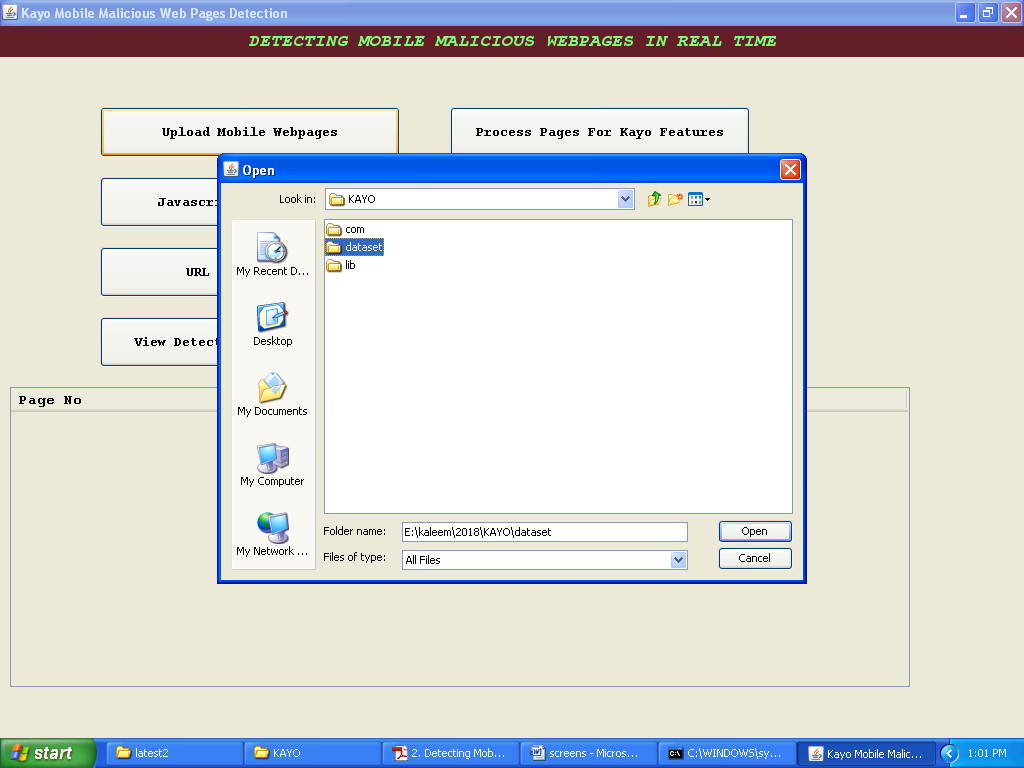
To implement this concept I downloaded some mobile webpages from internet and then apply above features technique to determine whether webpage is benign or malicious.

Dataset web pages are available inside dataset folder.

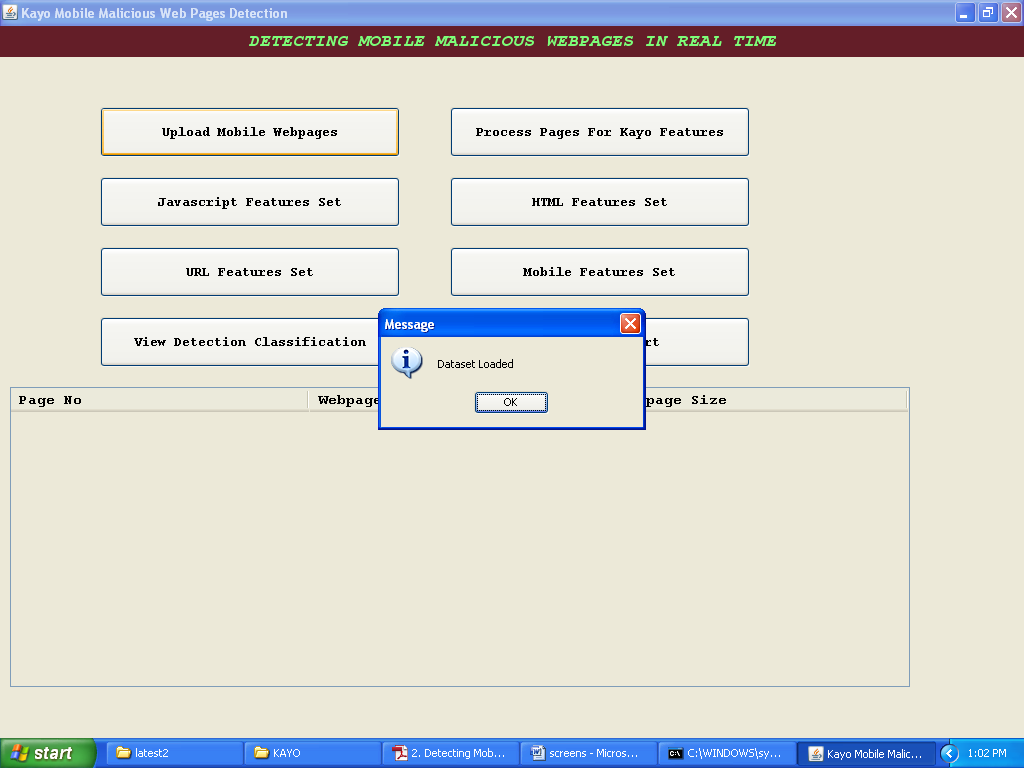
To execute project double click on ‘run.bat’ file to get below screen



Click on ‘Upload Mobile Webpages’ to upload entire dataset folder. This folder contains 12 web pages



After dataset upload will get below screen

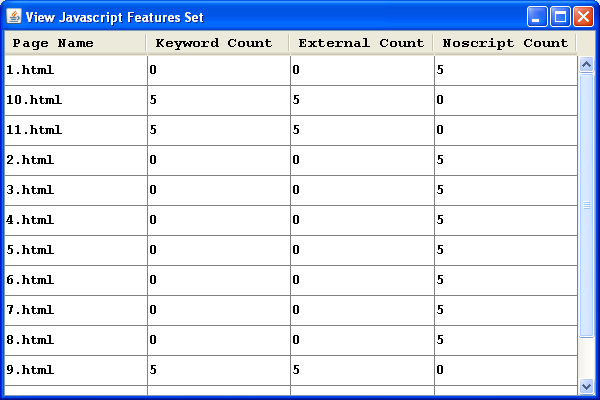


Now click on “Process Pages For Kayo Features’ to read dataset ant prepare processing features

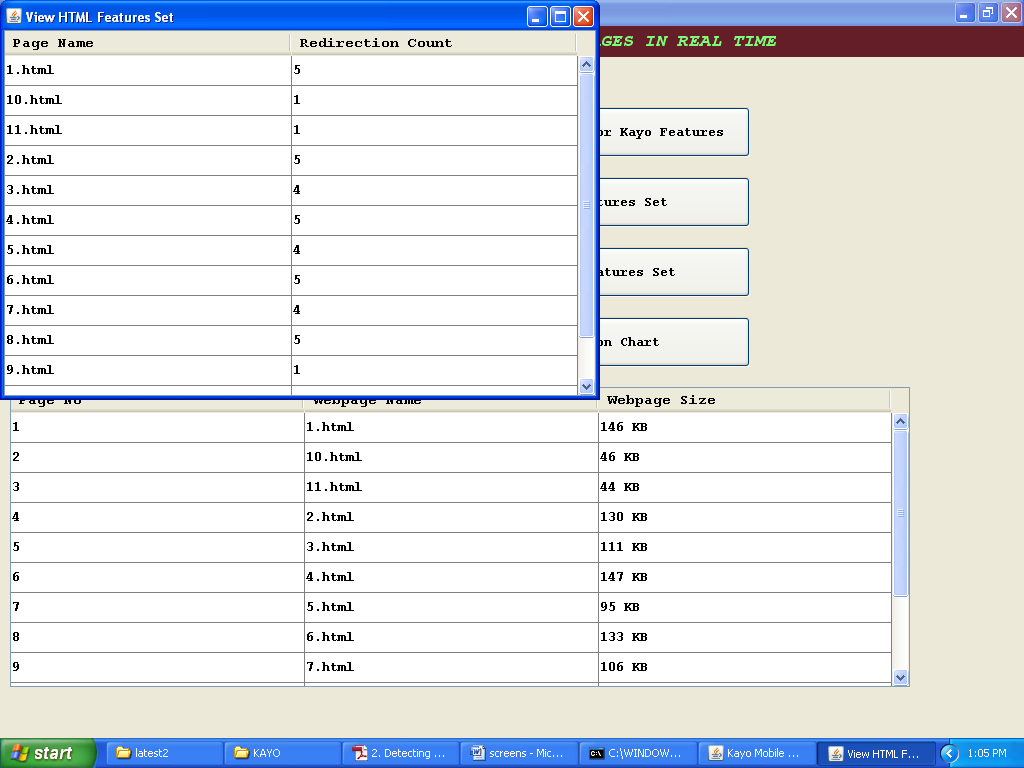


In above screen displaying process web page no, name and web page size.

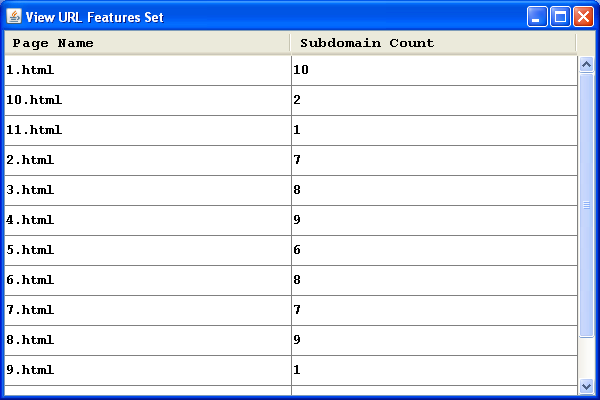
Now click on ‘Javascript Features Set’ to check for no of javascript tags used in web pages by web designer



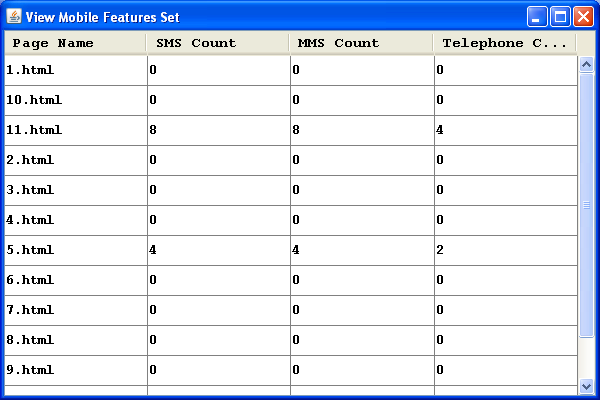
Now click on ‘HTML features set’ to get no of redirection pages used by web designer in webpage



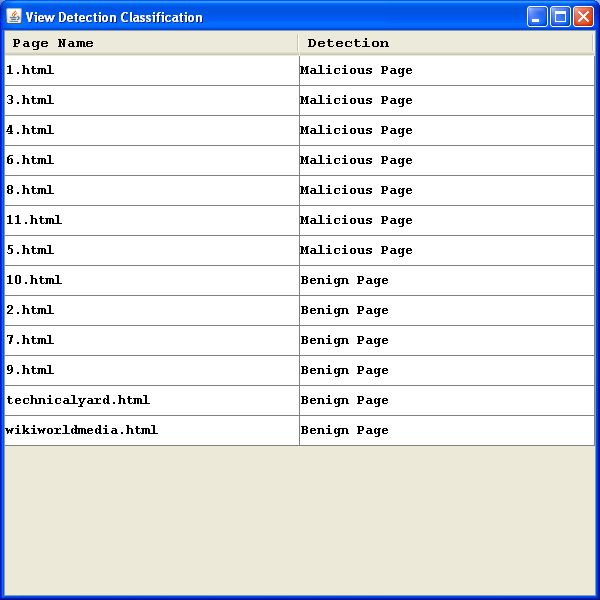
Now click on ‘URL features set’ to get no of sub domains used by web designer in web page



Now click on ‘Mobile features set’ to get no of time mobile api (mobile api such as sms, smsto, mms etc) used by web designer inside web page.



Now click on ‘View Detection Classification’ button to predict weather web page is malicious or not by analyzing above features count. If count > threshold then that page consider as malicious otherwise consider as benign.



Now click on ‘Detection Chart’ button to display graph for no of malicious and benign pages

