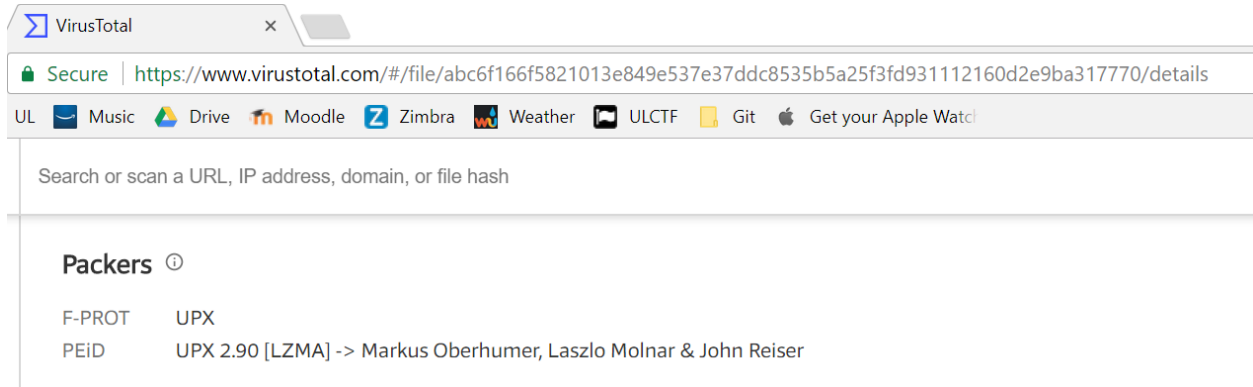


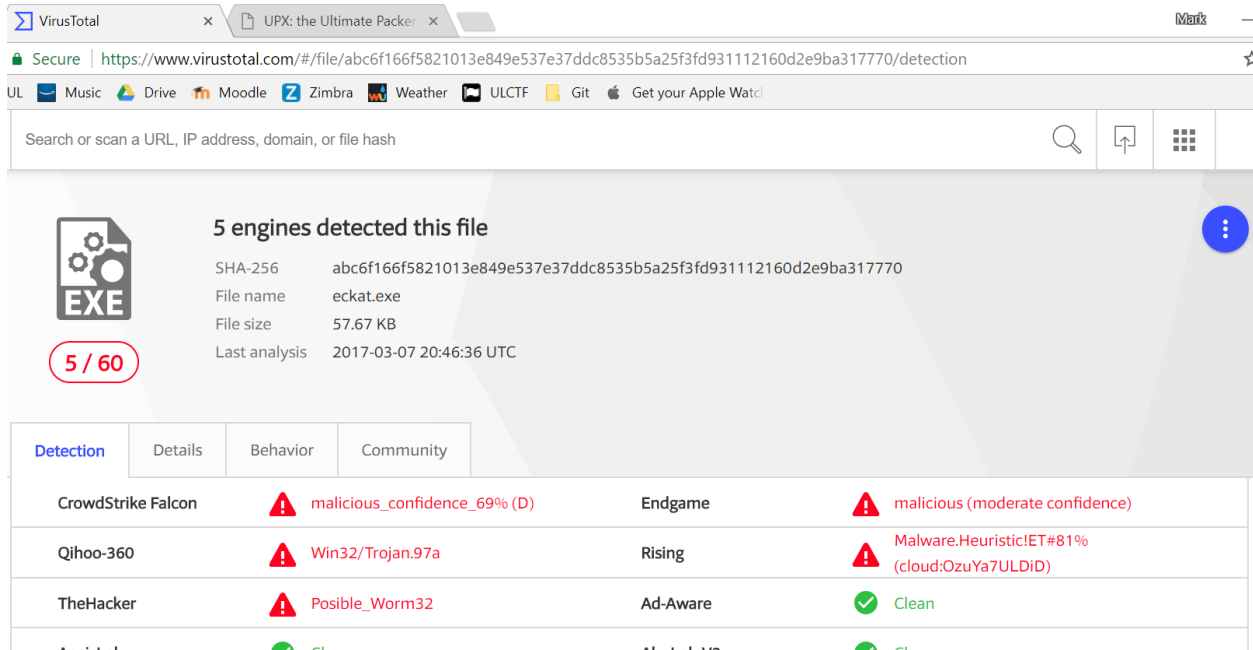
Assignment 7

3a. The file is packed using UPX - the Ultimate Packer for eXecutables.



The screenshot shows the VirusTotal details page for a file. The browser address bar displays the URL: <https://www.virustotal.com/#/file/abc6f166f5821013e849e537e37ddc8535b5a25f3fd931112160d2e9ba317770/details>. The page title is "Packers". The file is identified as being packed using UPX 2.90 [LZMA] -> Markus Oberhumer, Laszlo Molnar & John Reiser. The file name is "eekat.exe" and the file size is 57.67 KB. The last analysis was performed on 2017-03-07 20:46:36 UTC.

3b. 5 of 60 detected the file.



The screenshot shows the VirusTotal detection results for a file. The browser address bar displays the URL: <https://www.virustotal.com/#/file/abc6f166f5821013e849e537e37ddc8535b5a25f3fd931112160d2e9ba317770/detection>. The page title is "5 engines detected this file". The file is identified as being packed using UPX 2.90 [LZMA] -> Markus Oberhumer, Laszlo Molnar & John Reiser. The file name is "eekat.exe" and the file size is 57.67 KB. The last analysis was performed on 2017-03-07 20:46:36 UTC. The detection results show 5 engines detected the file as malicious, with a confidence of 69% (D). The engines are: CrowdStrike Falcon, Qihoo-360, TheHacker, and two others. The detection results are as follows:

Engine	Detection
CrowdStrike Falcon	malicious_confidence_69% (D)
Qihoo-360	Win32/Trojan.97a
TheHacker	Possible_Worm32
Abel_360	Clean
Abel_360	Clean

3c. The file makes get request to a site <http://eekat>. The user is probably not notified about this web requests or made aware of it.