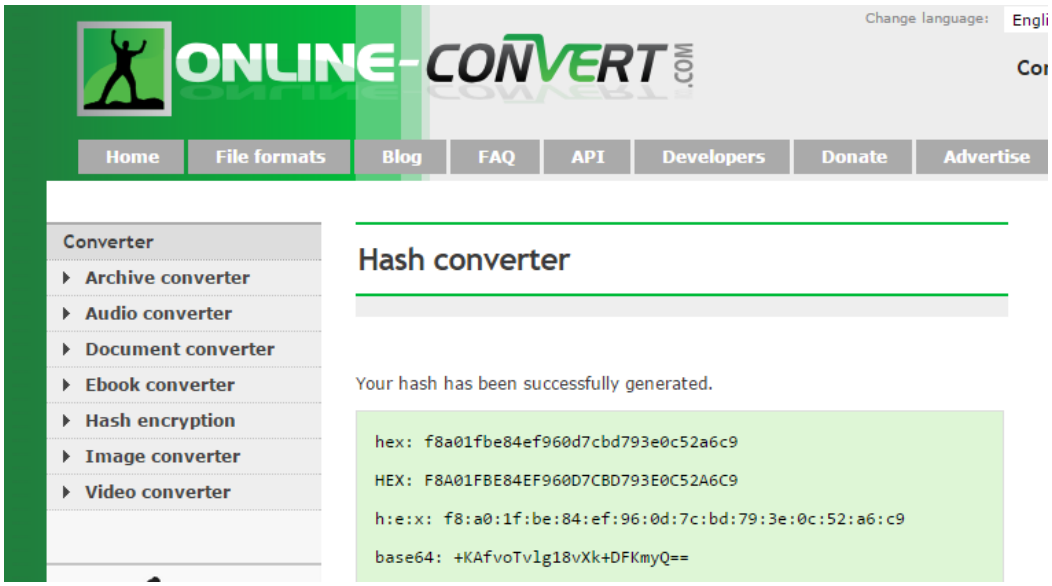
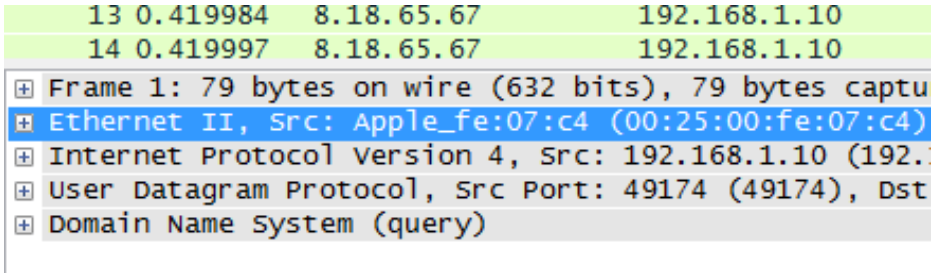
Networks Coursework

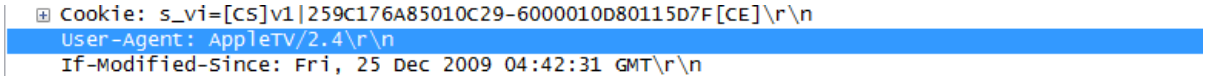
For the purpose of this assignment I was to take the role of a forensic investigator, investing suspicious activity of an employee and her newly acquired apple tv. I was presented with a pcap file containing evidence of the alleged suspicious activity and the md5 hash of the file in question. My first task was to check the md5 hash of the evidence and compare it to the md5 I was given to verify that the contents had not been altered in any way. To do this I used an online tool http://www.online-convert.com/. I uploaded the evidence file and then checked the md5 against the one I had been given, they matched so I continued with my investigation.



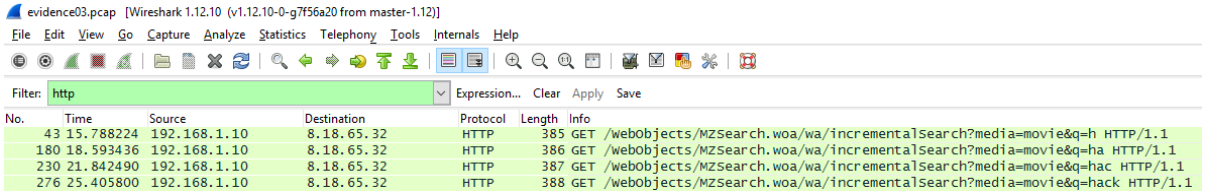
The tool I have used for the rest of my investigation is Wireshark. I loaded the evidence file into Wireshark so I could review the contents. I had been given the static IP address that had been used to configure the apple tv and was tasked with finding the mac address of the device. By filtering the evidence for http requests and the provided IP address I was able to determine that the mac address of the apple tv is (00:25:00:fe:07:c4).



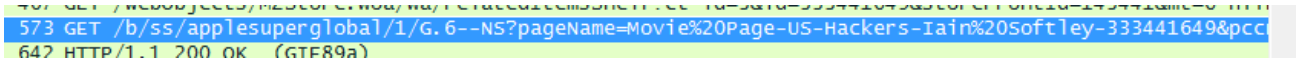
My next task was to find the user agent string used by the apple tv. To do this I again filtered the evidence by outgoing http requests. When viewing further information for the packets left I determined that the same user agent string was used for each request, AppleTV/2.4 and that this therefore must be the user agent string for the user being investigated.



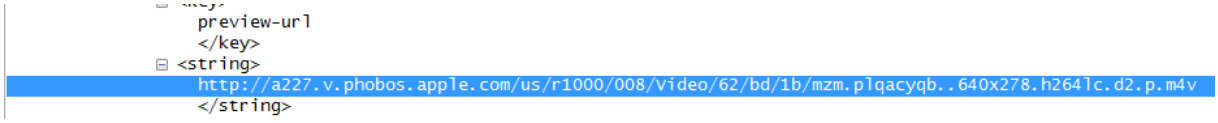
My next task was to find the first four terms the user searched for, including incremental searches. Incremental searches are automatically conducted after each letter is typed, the first four terms the user searched for were h, ha, hac and hack.



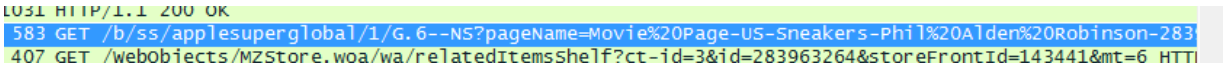
From here the user navigated to a movie. The title of this movie I can see from the http request is Hackers.



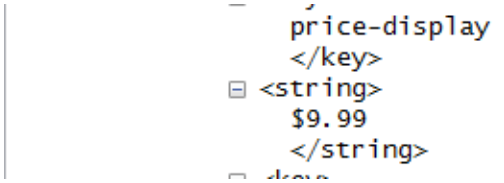
Near the packet containing this information was a html/xml packet. The xml contains more extensive data about the movie. By searching through this xml data I was able to find the heading preview-url and the full url for this movie trailer, the url being http://a227.v.phobos.apple.com/us/r1000/008/Video/62/bd/1b/mzm.plqacyqb..640x278.h264lc.d2.p.m4v.



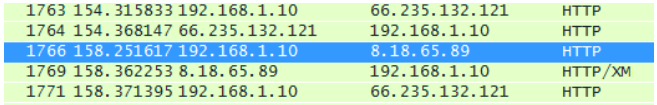
My next task was to find the second movie the user clicked on, having found the first one early in the packet data I knew the format I was looking for, by searching for the same format as the first movie I easily found the data for the second, the title of this movie was Sneakers.

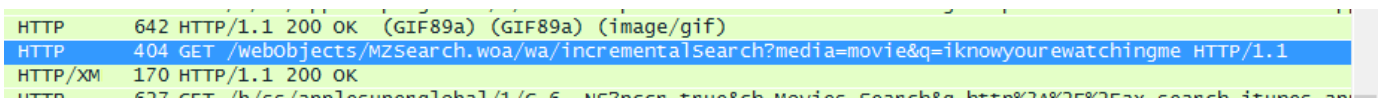


I then had to find out the cost to buy this movie, this was achieved in exactly the same way as the trailer url was found for the first movie, by searching the xml data for this movie and scrolling through the information I was able to determine the price was $9.99.



My final task was to find the final full term the user searched for, by again filtering by http requests and ordering the data by time I was able to find that the final full term searched for was: iknowyourewatchingme.





From my investigation I have determined that the activity is suspicious. The employee seems to be very aware of the investigation and is deliberately searching for terms to send messages to whoever may look at the data.