***Week 8: Static Malware analysis   
Tools/Utility used- Text Edito*r**  
Q. What is the text present as part of email when the victim receives this malware?

I hate to go to school  
Q. What is the domain name that was added as the browser’s homepage?

http://www.skyinet.net  
Q. The malware replicated itself into 3 locations, what are they?

System, tmp and windows  
Q. What is the name of the file that looks for the filesystem?

Q. Which file extensions, beginning with m, does this virus target?

.mp3,.mp2  
Q. What is the name of the file generated when the malware identifies any Internet Relay Chat service?

LOVE-LETTER-FOR-YOU.HTM  
Q. What is the name of the password stealing trojan that is downloaded by the malware?

barok  
Q. What is the name of the email service that is targeted by the malware?

outlook  
Q. What is the registry entry responsible for reading the contacts of the logged in email account?

HKEY\_CURRENT\_USER\Software\Microsoft\WAB\  
Q. What is the value that is stored in the registry to remember that an email was already sent to a user?

1