Scenario *ILOVEYOU: the three magical words that have an impact on most of people's lives.*
On the other hand, these three words need no introduction for people in the Infosec industry.

Let's relive history by analyzing the 'ILOVEYOU' malware.

This challenge should be completed in a virtual machine as it contains real malware.

1. What is the text present as part of the email when the victim received this malware?

- Format: `Email Body Text`

2. What is the domain name that was added as the browser's homepage?

- Format: `http://www.domain.tld/`

3. The malware replicated itself into 3 locations, what are they?

- Format: `C:\Windows\System32\filename.ext, C:\Windows\System32\filename.ext, C:\Windows\filename.ext`

4. What is the name of the file that looks for the filesystem?

- Format: `filename.extension`

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

- Format: `ext1, ext2`

6. What is the name of the file generated when the malware identifies any Internet Relay Chat service?

- Format: `filename.extension`

7. What is the name of the password-stealing trojan that is downloaded by the malware?

- Format: `Trojan Name`

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

- Format: `Email Service Targeted`

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

- Format: `registry\key\name\`

10. What is the value that is stored in the registry to remember that an email was already sent to a user?

- Format: `Registry Value`