404 Not Found - Isn't that a Mystery?!

Download the following ZIP file (password: infected):

404 Not Found (791 KB)

The attached PCAP file captures the activity of a machine infected with an unknown malware. Your task is to analyze the events, construct an infection timeline, and provide detailed documentation using the following prompts:

1. Identify the victim machine: Include its name, MAC address, and operating system.
2. Describe the infection process: Outline each stage of the attack chain leading to the machine's compromise.
3. Initial post-infection activities: Detail any network reconnaissance or downloads of additional code or executables.
4. Communication with external servers: Note any connections to Command-and-Control (C2/CnC) servers and list relevant IP addresses or domains.
5. Malicious actions done by the malware: Document the harmful activities carried out by the malware on the infected machine.
6. Extraction of malware samples: Attempt to extract any malware samples present in the PCAP for further analysis.

Keep in mind:

- Extract and analyze specific traffic segments crucial to understanding the attack progression.
- Record your findings systematically to facilitate a comprehensive analysis of the malware infection.