Automated eForensics system

Description:
Design an automated eforensics system that will conduct a eforensics diagnostics against a mounted drive and generate a report.

Functional requirements:

- Mount the common eforensic file formats including E01, DD, LEF (l01), ZIP, and DMG
- Create a MD5 hash of the drive
- Check and verify MD5 and SHA1 hashes of files
- Check all file for:
  - Undeleted files
  - Renamed files
  - Carved files
  - Identify file content headers i.e. zip files commonly use the “PK” header
  - Scan for keywords within files relevant to the investigation
- Generate a report with the findings:
  - Build an event timeline of the findings
    - When was the last time files were modified
    - How was it changed (if possible)
    - Retrace file location manipulation (if possible)
  - List all suspicious files and their MAC dates
  - Suspicious file details including:
    - File Name
    - iNode Number
    - Modified Date
    - Accessed Date
    - Created Date
    - File Size
    - MD5 hash of the files
  - Timezone of the user and computer time (if possible)

Optional functional requirements:

- Create an eforensics file from a physical drive (i.e. USB)
- Memory forensics
  - Create an eforensics file for the memory
  - Dump current memory into eforensics file
  - Check for suspicious activity
- Scan email content for suspicious attachments or keywords