Spies Like Us

Evidence Available

You are provided with the following evidence -

- Forensic image of Klaus Fuchs' computer
    - 17APR DD Case.001 – 006
- Autopsy and Bulk Extractor Reports
- Encrypted containers
    - Vacation Pics.zip
    - Outdoor Pics.zip

Information regarding the encrypted containers

- Vacation Pics.zip
    - Single volume:
        - Keyfile - The picture attached to an email Klaus received from Aldrich on 10 APR 20 at 14:48 CT
        - Password - The public IPv4 address associated with an encrypted email sent from Aldrich to Klaus on 10 APR 20 at 14:59 CT
- Outdoor Pics.zip
    - Outer volume:
        - Keyfile - File stored within Vacation Pics.zip container. The word "KEYFILE" is in the file name in all capital letters.
        - Password - The last write time (UTC) of the Local Area Connection* 2 interface as listed in the registry.
    - Inner Volume:
        - Keyfile - File stored within the outer volume of Outdoor Pics.zip
        - Password - The quote at the end of the encrypted email that Klaus received from Aldrich on 10 APR 20 at 14:59 CT.

Your end goal is to analyze the evidence available and answer the following questions:

- Question 1 – What is the public IP address associated with an encrypted email sent from Aldrich to Klaus on 10 APR 20 at 14:59 CT? Enter all four (4) octets in dot-decimal notation (e.g., 123.45.67.89).
- Question 2 – What is the last write time (UTC) of the Local Area Connection* 2 interface as listed in the registry? Enter the hours, minutes, and seconds for the password/submission, including colons (e.g., 01:02:03).

- Question 3 – What is the quote at the end of the encrypted email that Klaus received from Aldrich on 10 APR 20 at 14:59 CT? There are no capital letters, punctuation, or spaces in the password (e.g., haveaniceday).
- Question 4 – What is the hashtag label listed on the file within the hidden container of Outdoor Pics.zip? Include the hashtag symbol followed by the word(s) without any spaces (e.g., #wintheday).