Digital Forensic Investigation Report

1. Case Details

- **Case Title:** Analysis of Suspected Disk Image
- **Investigator Name:** Nick • **Date of Analysis:** 31/08/2025
- **Tools Used:** ○ BEViewer ○ Bulk Extractor ○ Windows PowerShell (for hash verification)

2. Objective

To examine the provided forensic disk image and extract potential evidence such as emails, URLs, telephone numbers, or other artifacts using forensic tools.

3. Evidence Acquisition

- **Image File Analyzed:** terry-work-usb-2009-12-11 (3).E01
- **Source:** Provided as a raw forensic image
- **Mounting:** Directly analyzed without using an image mounting tool
- **Image Details:**

  Evidence File Path: D:\FORENSIC\terry-work-usb-2009-12-11 (3).E01

  Image Format: E01 (EnCase) Image Size:

  31.9 MB (33,499,203 bytes)

- **Hash Verification:**

Hash Algorithm	Hash Value
MD5	941997B1B9E7A1217351D483C12DC29B
SHA1	7709ECA151DAA2BAA1DB258DDB74432D540793AD

Hash Verification Time: 31 July 2025, 11:25 PM

Tool Used: Get-FileHash in Windows PowerShell

4. Analysis Process

Step 1: Opened the image file in **BEViewer**
Step 2: Launched **Bulk Extractor** from within BEViewer (Tools > Run Bulk Extractor)
Step 3: Selected the image file for scanning
Step 4: Enabled the following scanners for artifact extraction:

- email
- httplogs
- json
- pdf
- net
- vcard
- exif
- base64
  ...and others as required.

System Environment: Windows 10 x64 (Host: Chainsmokers)

Bulk Extractor Version: 1.5.0

5. Findings

- Total Telephone Numbers Extracted: 3

- Total URLs Extracted: 5

- **URLs Found:**
  - http://memory.loc.gov/ammem/award99/cubhtml/copyres.ht
  ml ○ http://www.ars-grin.gov/misc/mmpnd/Kalopanax.html
  - http://www2.cdc.gov/phlp/docs/661506.pdf
  - http://www.hhs.gov/ohr/eap/newsletter/summer05.pdf ○
    http://thomas.loc.gov/home/gpoxmlc111/hr867_eh.xml
- **Telephone Found:**

S.No.	Telephone Number	Source File Path / Context
1	177-188-1984	chives/techbull/177-188-1984.pdf
2	118/150/1746	filestorage/78/118/150/1746/… (format unclear)

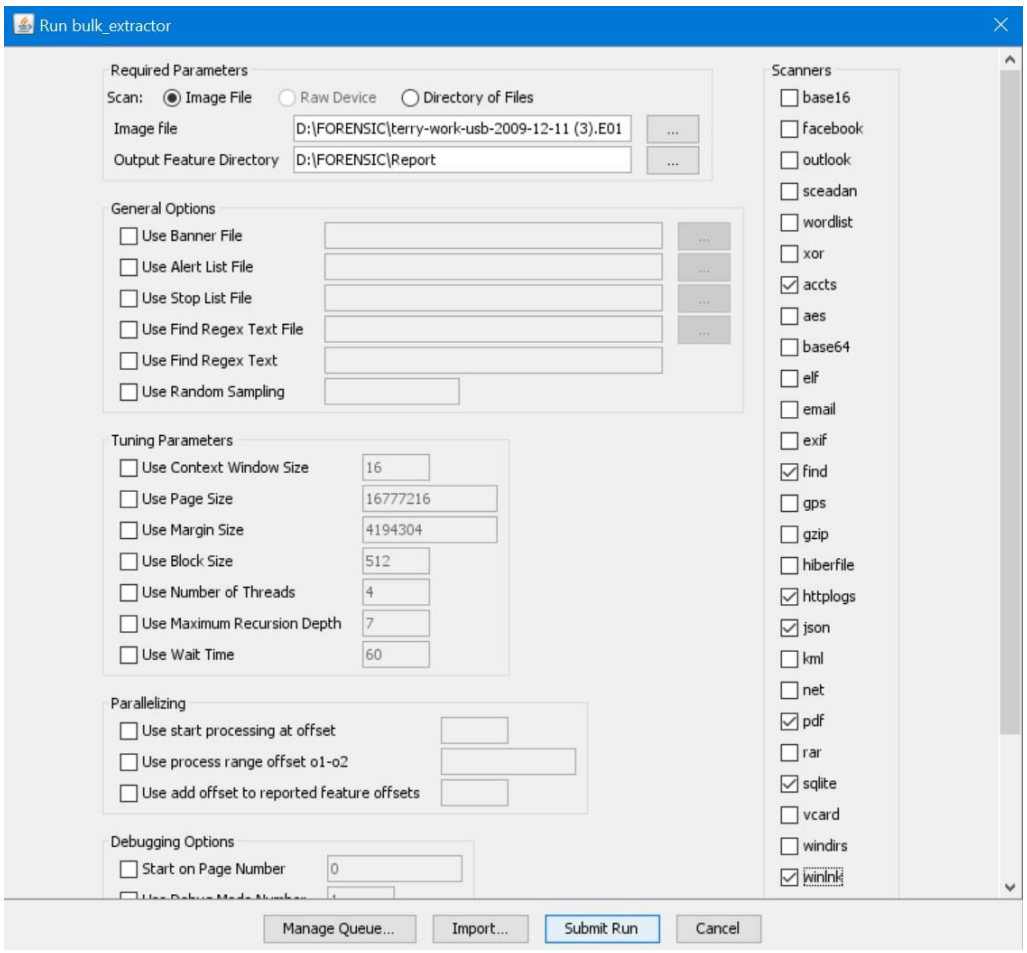
3 600/370-7924 usgs-manual/370-600/370-7924.html

Output Directory Location: D:\FORENSIC\Report

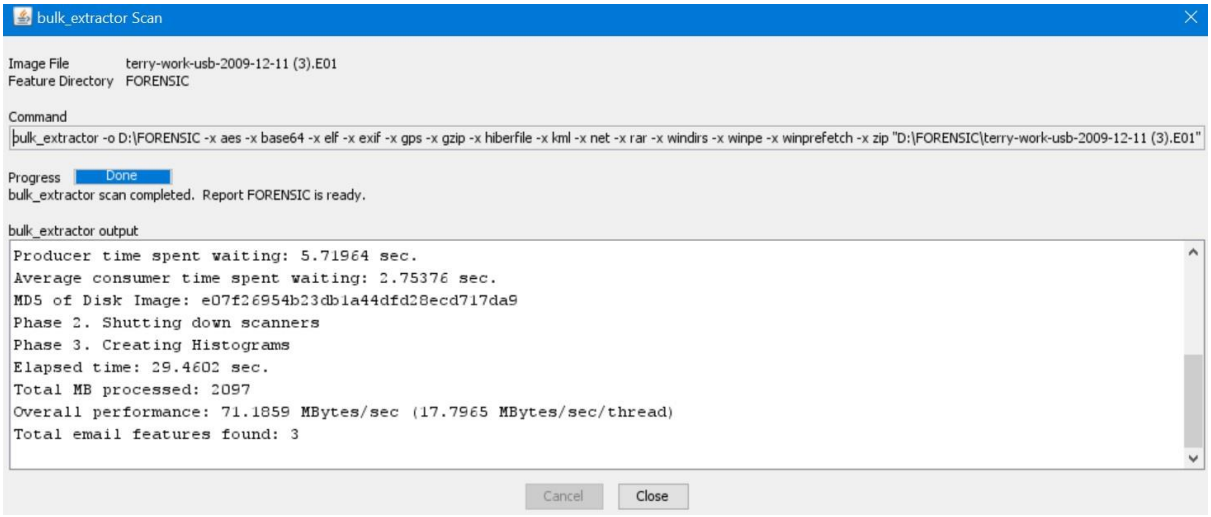
6. Screenshots

- Bulk Extractor GUI with selected scanners and result window

  Captured: 31 July 2025, 11:12 PM

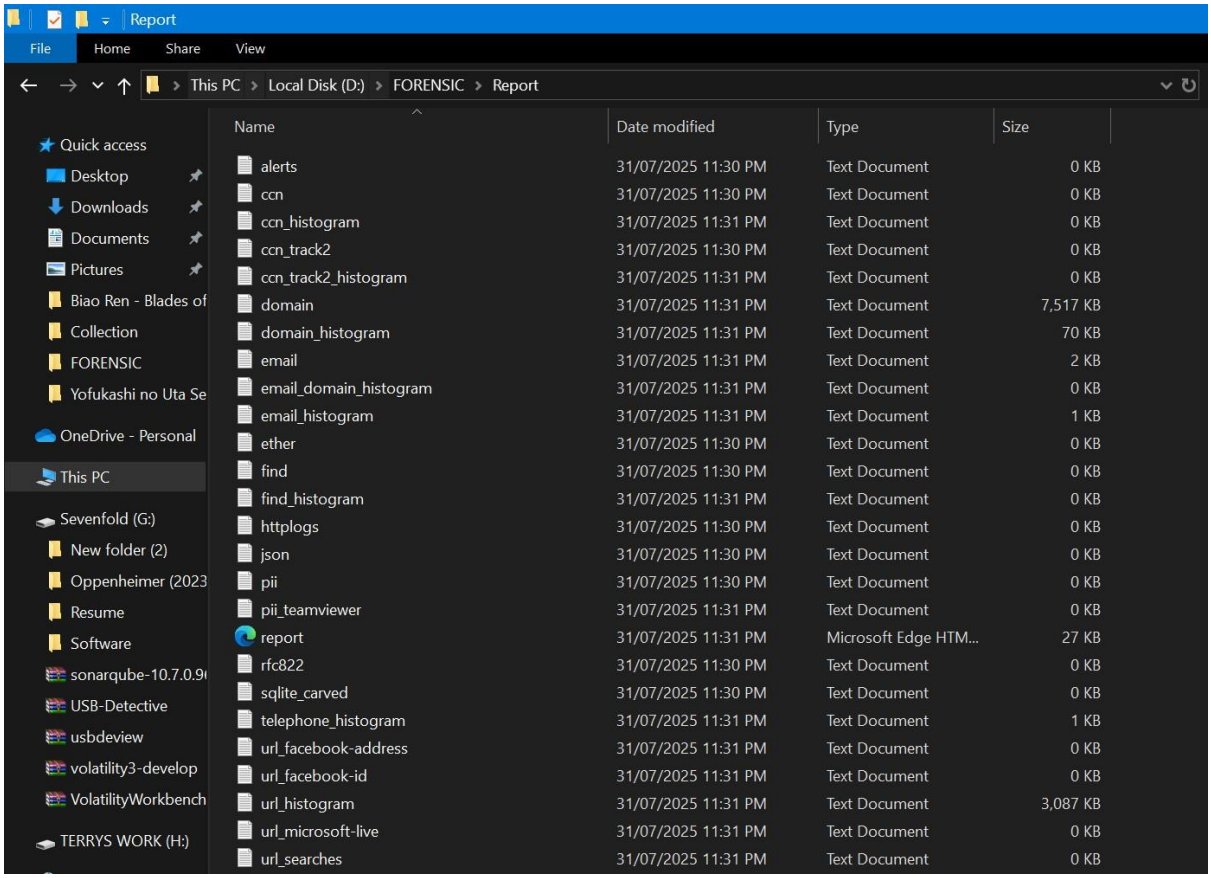


Captured: 31 July 2025, 11:13 PM

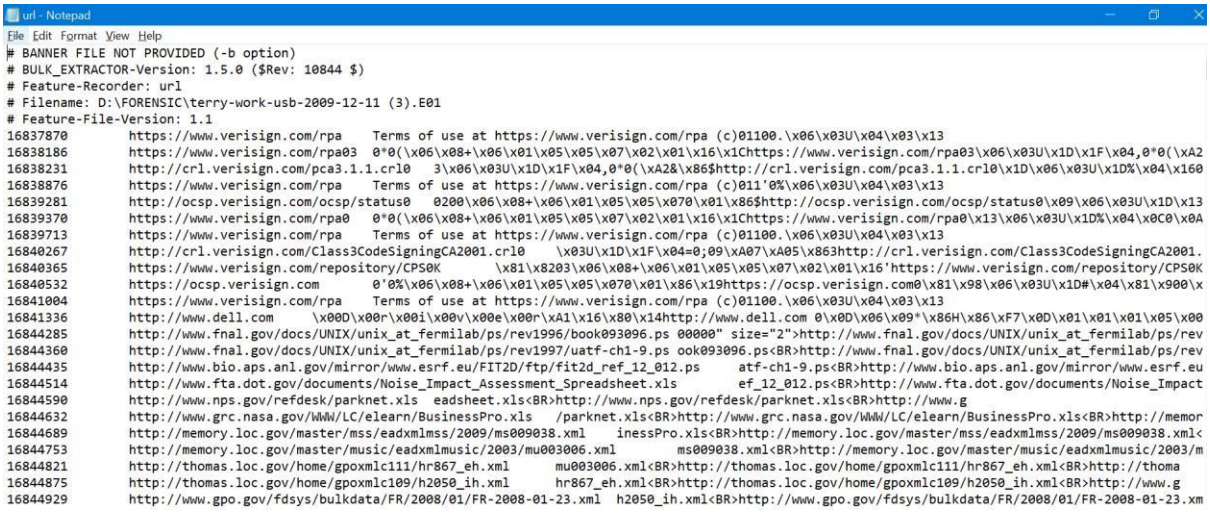


- Output directory and any open result files

  Captured: 31 July 2025, 11:15PM

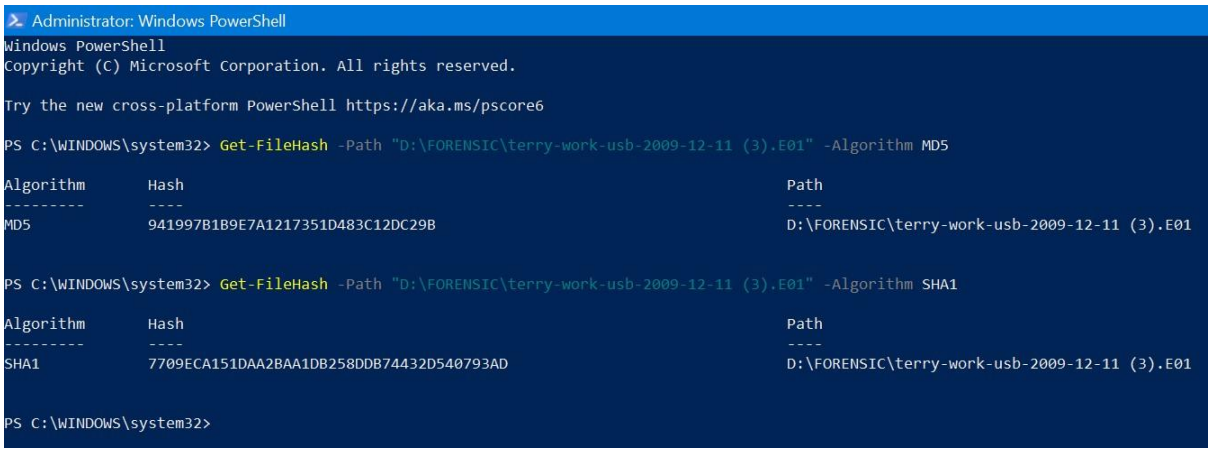


Captured: 31 July 2025, 11:15 PM



- PowerShell window showing hash output

  Captured: 31 July 2025, 11:05 PM



8. **Conclusion**

The forensic investigation was successfully completed on the provided disk image using Bulk Extractor and other relevant tools. All analysis steps were conducted systematically, and the integrity of the evidence was maintained throughout. Required artifacts such as URLs and telephone numbers were successfully extracted.