

# 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.html>
- <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](http://thomas.loc.gov/home/gpoxmlc111/hr867_eh.xml)

- **Telephone Found:**

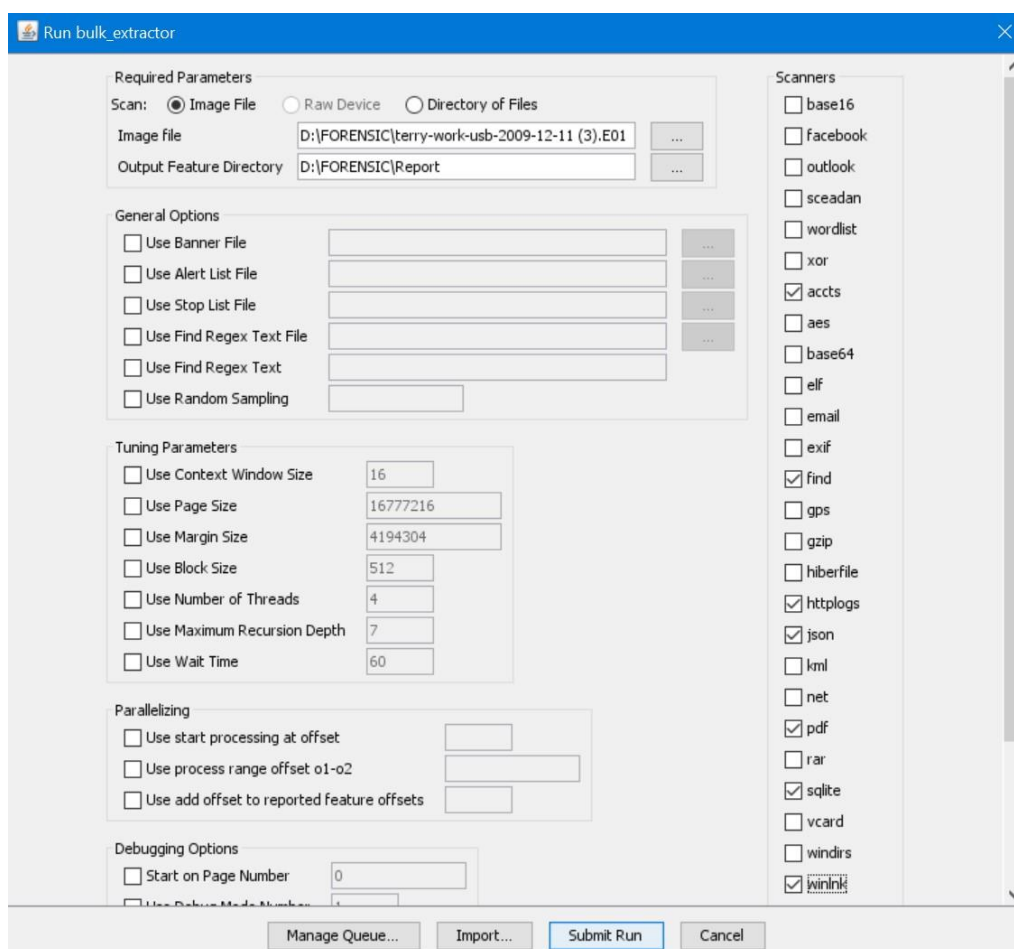
S.No.	Telephone Number	Source File Path / Context
1	177-188-1984	chives/techbull/177-188-1984.pdf
2	118/150/1746	filestorage/78/118/150/1746/... (format unclear)

**Output Directory Location:** D:\FORENSIC\Report

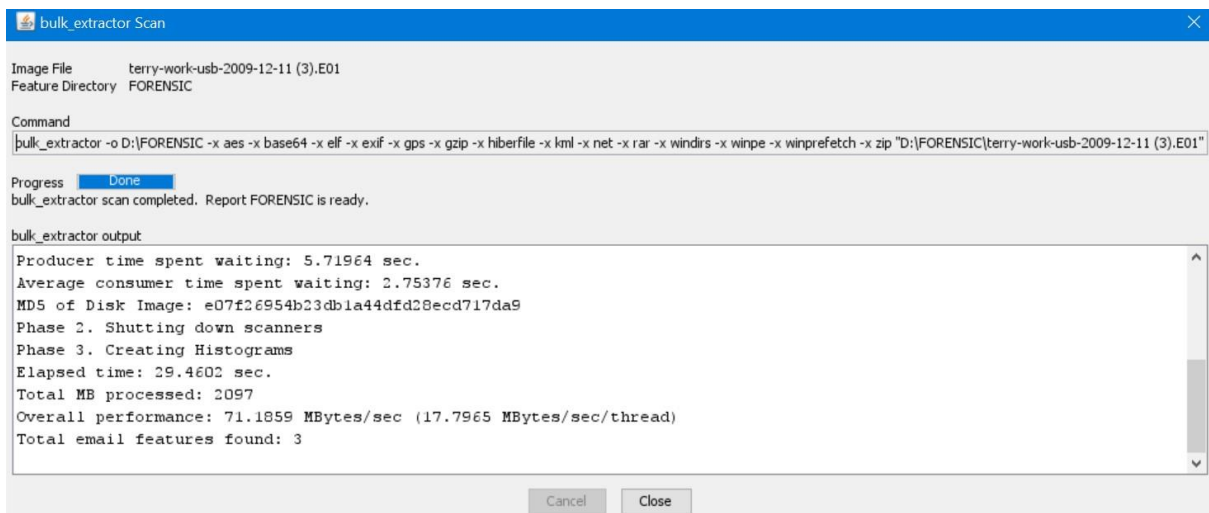
## 6. Screenshots

- Bulk Extractor GUI with selected scanners and result window

Captured: 31 July 2025, 11:12 PM

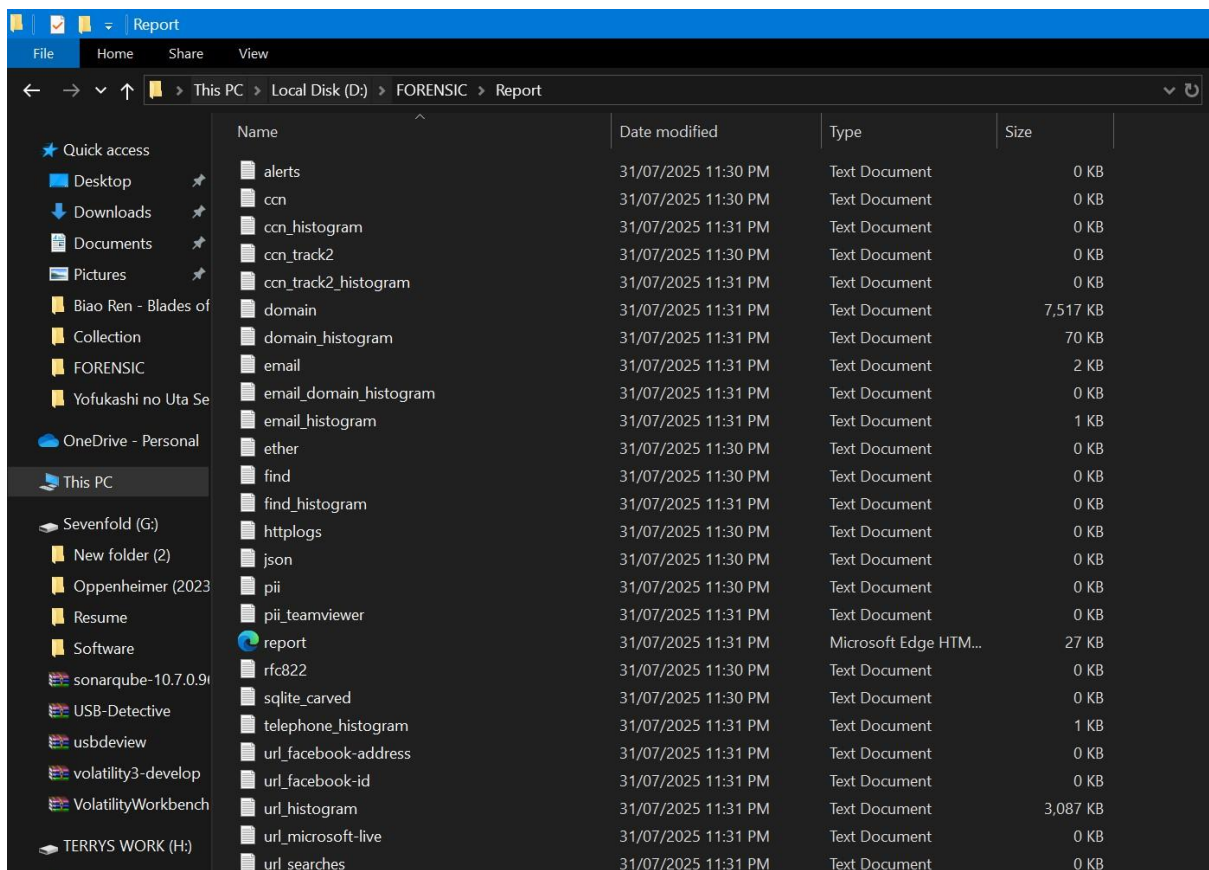


Captured: 31 July 2025, 11:13 PM



- Output directory and any open result files

Captured: 31 July 2025, 11:15PM



Captured: 31 July 2025, 11:15 PM

```

url - Notepad
File Edit Format View Help
# BANNER FILE NOT PROVIDED (-b option)
# BULK_EXTRACTOR-Version: 1.5.0 ($Rev: 10844 $)
# Feature-Recorder: url
# Filename: D:\FORENSIC\terry-work-usb-2009-12-11 (3).E01
# Feature-File-Version: 1.1
16837870 https://www.verisign.com/rpa Terms of use at https://www.verisign.com/rpa (c)01100.\x06\x03U\x04\x03\x13
16838186 https://www.verisign.com/rpa03 0*0(\x06\x08+\x06\x01\x05\x05\x07\x02\x01\x16\x1Chttps://www.verisign.com/rpa03\x06\x03U\x1D\x1F\x04,0*0(\xA2
16838231 http://cr1.verisign.com/pca3.1.1.cr10 3\x06\x03U\x1D\x1F\x04,0*0(\xA2&\x86$https://cr1.verisign.com/pca3.1.1.cr10\x1D\x06\x03U\x1D\x04\x160
16838876 https://www.verisign.com/rpa Terms of use at https://www.verisign.com/rpa (c)011'0%\x06\x03U\x04\x03\x13
16839281 http://ocsp.verisign.com/ocsp/status0 0200\x06\x08+\x06\x01\x05\x05\x070\x01\x86$https://ocsp.verisign.com/ocsp/status0\x09\x06\x03U\x1D\x13
16839370 https://www.verisign.com/rpa0 0*0(\x06\x08+\x06\x01\x05\x05\x07\x02\x01\x16\x1Chttps://www.verisign.com/rpa0\x13\x06\x03U\x1D\x04\x0C0\x0A
16839713 https://www.verisign.com/rpa Terms of use at https://www.verisign.com/rpa (c)01100.\x06\x03U\x04\x03\x13
16840267 http://cr1.verisign.com/Class3CodeSigningCA2001.cr10 \x03U\x1D\x1F\x04=0;09\xA07\xA05\x863https://cr1.verisign.com/Class3CodeSigningCA2001.
16840365 https://www.verisign.com/repository/CP50K \x81\x8203\x06\x08+\x06\x01\x05\x05\x07\x02\x01\x16'https://www.verisign.com/repository/CP50K
16840532 https://ocsp.verisign.com 0'0%\x06\x08+\x06\x01\x05\x05\x070\x01\x86\x19https://ocsp.verisign.com0\x81\x98\x06\x03U\x1D#\x04\x81\x900\x
16841004 https://www.verisign.com/rpa Terms of use at https://www.verisign.com/rpa (c)01100.\x06\x03U\x04\x03\x13
16841336 http://www.dell.com \x00D\x00r\x00i\x00v\x00e\x00r\xA1\x16\x80\x14http://www.dell.com 0\x0D\x06\x09*\x86H\x86\xF7\x0D\x01\x01\x01\x05\x00
16844285 http://www.fnal.gov/docs/UNIX/unix_at_fermlab/ps/rev1996/book093096.ps 00000" size="2">http://www.fnal.gov/docs/UNIX/unix_at_fermlab/ps/rev
16844360 http://www.fnal.gov/docs/UNIX/unix_at_fermlab/ps/rev1997/uatf-ch1-9.ps ook093096.ps<BR>http://www.fnal.gov/docs/UNIX/unix_at_fermlab/ps/rev
16844435 http://www.bio.aps.anl.gov/mirror/www.esrf.eu/FIT2D/ftp/fit2d_ref_12_012.ps atf-ch1-9.ps<BR>http://www.bio.aps.anl.gov/mirror/www.esrf.eu
16844514 http://www.fta.dot.gov/documents/Noise_Impact_Assessment_Spreadsheet.xls ef_12_012.ps<BR>http://www.fta.dot.gov/documents/Noise_Impact
16844590 http://www.nps.gov/refdesk/parknet.xls eadsheet.xls<BR>http://www.nps.gov/refdesk/parknet.xls<BR>http://www.g
16844632 http://www.grc.nasa.gov/WWW/LC/elearn/BusinessPro.xls /parknet.xls<BR>http://www.grc.nasa.gov/WWW/LC/elearn/BusinessPro.xls<BR>http://memor
16844689 http://memory.loc.gov/master/mss/eadxmlmss/2009/ms009038.xml inessPro.xls<BR>http://memory.loc.gov/master/mss/eadxmlmss/2009/ms009038.xml<
16844753 http://memory.loc.gov/master/music/eadxmlmusic/2003/mu003006.xml ms009038.xml<BR>http://memory.loc.gov/master/music/eadxmlmusic/2003/m
16844821 http://thomas.loc.gov/home/gpoxmlc111/hr867_eh.xml mu003006.xml<BR>http://thomas.loc.gov/home/gpoxmlc111/hr867_eh.xml<BR>http://thoma
16844875 http://thomas.loc.gov/home/gpoxmlc109/h2050_ih.xml hr867_eh.xml<BR>http://thomas.loc.gov/home/gpoxmlc109/h2050_ih.xml<BR>http://www.g
16844929 http://www.gpo.gov/fdsys/bulkdata/FR/2008/01/FR-2008-01-23.xml h2050_ih.xml<BR>http://www.gpo.gov/fdsys/bulkdata/FR/2008/01/FR-2008-01-23.xm

```

- PowerShell window showing hash output

Captured: 31 July 2025, 11:05 PM

```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> Get-FileHash -Path "D:\FORENSIC\terry-work-usb-2009-12-11 (3).E01" -Algorithm MD5

Algorithm      Hash                                                    Path
-----
MD5            941997B1B9E7A1217351D483C12DC29B                    D:\FORENSIC\terry-work-usb-2009-12-11 (3).E01

PS C:\WINDOWS\system32> Get-FileHash -Path "D:\FORENSIC\terry-work-usb-2009-12-11 (3).E01" -Algorithm SHA1

Algorithm      Hash                                                    Path
-----
SHA1           7709ECA151DAA2BAA1DB258DDB74432D540793AD            D:\FORENSIC\terry-work-usb-2009-12-11 (3).E01

PS C:\WINDOWS\system32>

```

## 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.