Cyberster

INTERNSHIP REPORT

A Weekly Progress and Learning Summary

Phase Two : Autopsy Triage, Artifact Hunting, and Registry Analysis

Submitted to: Cyberster Internship Program

Intern Name: Abdul Muqeet Tabraiz

Roll Number: CSI-B1-353

Autopsy Triage | File System Analysis | Artifact Hunting | Keyword Search
Registry Hive Analysis | Key & Value Analysis | Cross-Artefact Correlation

A Weekly Progress and Learning Summary

Table of Contents

Overall Assessment of Mantooth Activity

Evidence Connecting Mantooth to Fraudulent Cheques

Leads to Follow Next

Gaps and Limitations

Week 10 Conclusion

Week 10 Overview

Week 10 of the Cyberster Blue Team Internship represents the most ambitious deliverable of Phase Two so far. The week consolidates every disk-image, registry, and Windows-artefact skill developed across Weeks 7 to 9 into a single end-to-end investigation against the Mantooth.E01 forensic image — a real-world fraudulent-cheque case targeting suspect Wes Mantooth. The deliverable is a fully bookmarked Autopsy case, a parsed registry workbook, and a written investigative commentary that connects the artefacts to the alleged criminal conduct.

Part A (Days 67 to 69) covers Autopsy Triage and Windows Artifact Hunting. The Mantooth.E01 image is ingested with Mountain Time (America/Denver) as the case timezone. After ingest the examiner answers fourteen investigative questions covering image integrity, partition layout, EXIF metadata, encryption indicators, deleted-file recovery, web-search history, IP and email extraction, user accounts, thumbcache reconstruction, Recycle Bin contents (Camerashy.exe), Prefetch analysis with PECmd (XCOPY.EXE), LNK parsing with LECmd, print spool analysis, and Security event log session reconstruction with EvtxECmd.

Part B (Days 70 to 73) covers Windows Registry Analysis. The SYSTEM, SOFTWARE, SAM, SECURITY, and NTUSER.DAT hives are extracted from the image and loaded into Eric Zimmerman's Registry Explorer to answer thirty-four registry-only questions covering computer name, timezone, hard-drive identification, DHCP configuration, Prefetch state, the TrueCrypt service, last-shutdown time, network adapters, wireless profiles, OS registration, USB device enumeration with drive-letter correlation, profile and SAM account analysis, the WinVNC password, Yahoo Messenger username, installed software with timestamps, MRU lists for Adobe Reader / Paint / PowerPoint / Media Player / RecentDocs / RunMRU, default printer and browser configuration, IE start page and download directory, IE favourites and TypedURLs, and a cross-hive email address sweep.

Part C is the investigative commentary that synthesises every artefact into a cohesive narrative connecting Mantooth to the alleged fraudulent-cheque scheme — using the TrueCrypt encryption service, the Camerashy.exe steganography tool found in the Recycle Bin, the ATM_THEFTS1.ppt registry trace, Xcopy Prefetch evidence, and the F: drive Windows Media Player history — and identifies the next investigative leads as well as the gaps and limitations of the current evidence set.

Critical Discipline Followed All Week: Mountain Time (America/Denver) was set on the data source BEFORE clicking Next so that every Autopsy timestamp shown in the report is in the image's native local timezone. Ingest was started on the morning of Day 67 and allowed to complete uninterrupted for approximately three hours; cancelling ingest mid-run is the single most destructive operator error in Autopsy work and would have forced a complete case rebuild.

Hash Discipline: The Data Source Integrity module computed the MD5 of Mantooth.E01 and matched it against the embedded E01 hash; the verification result is recorded as the very first investigative deliverable (Q1) and quoted verbatim from the Autopsy log into the evidence register below.

Bookmark Discipline: Every primary finding (Olympus EXIF photo, encrypted .doc, deleted HARDCORE.jpg / pfah603.jpg, Camerashy.exe in $Recycle.Bin, Xcopy Prefetch, ATM_THEFTS1.ppt, and the TrueCrypt service entry) was tagged inside Autopsy as it was discovered. This made the Generate Report step at the end of the week deterministic and ensured that no finding was overlooked when the report was assembled.

Part A — Autopsy Triage and Windows Artifact Hunting (Days 67–69)

Objective

The objective of Part A was to perform an end-to-end forensic triage of the Mantooth.E01 evidence image using Autopsy 4.21. The triage was required to verify image integrity, enumerate the partition layout, and answer fourteen sequential investigative questions ranging from EXIF metadata and encryption indicators through deleted-file recovery, web-search history, IP/email extraction, Recycle Bin reconstruction, Prefetch and LNK parsing with Eric Zimmerman's command-line tools, print spool extraction, and Security event log session reconstruction. Every finding was bookmarked in Autopsy as it was made, and every command line and tool output was preserved for evidentiary chain-of-custody.

Tools Used

- Autopsy 4.21 (sleuthkit.org/autopsy) — Primary triage platform; ingest modules, keyword search, EXIF, Email, Recent Activity, Recycle Bin parsing
- FTK Imager — Independent MD5 verification of the E01 image (cross-tool corroboration)
- PECmd.exe (Eric Zimmerman) — Windows Prefetch (.pf) parser with run-count, last-run, file-reference and volume metadata
- LECmd.exe (Eric Zimmerman) — LNK file parser exporting TargetCreated / TargetModified / TargetAccessed, VolumeSerialNumber, DriveType, MachineID and TargetIDAbsolutePath
- EvtxECmd.exe (Eric Zimmerman) — Windows Event Log parser converting Security.evtx into structured CSV with mapped EventID / Channel / Provider / Payload data
- Thumbcache Viewer (thumbcacheviewer.github.io) — Renders thumbcache_*.db entries to disk for visual review
- Microsoft Excel — Filtering, sorting, MISSING TARGET / LOGON SESSION annotation, CSV pivot

Phase 0 — Tooling and Environment Preparation

Step 1: Download Required Forensic Toolkit

All required Week 10 tools were downloaded prior to Day 67 and extracted to C:\Forensics\Tools\. No installer was used for the Eric Zimmerman utilities — they ship as standalone binaries and were run from their extracted folders. Autopsy was installed via its official MSI.

Tool	Source	Used In
Autopsy 4.21	sleuthkit.org/autopsy	Days 67–73 (both parts)
Registry Explorer 2026.5.0	ericzimmermann.com/tools	Part B Days 70–73
PECmd 2026.5.0	ericzimmermann.com/tools	Part A Q11 (Xcopy Prefetch)
LECmd 2026.5.0	ericzimmermann.com/tools	Part A Q12 (LNK parsing)
EvtxECmd 2026.5.0	ericzimmermann.com/tools	Part A Q14 (Security log)
Thumbcache Viewer	thumbcacheviewer.github.io	Part A Q9
FTK Imager	exterro.com	Independent MD5 verification

Step 2: Working Folder Layout

A flat working tree was created under C:\Forensics\Week10\ to hold the case file, exported artefacts, parsed CSVs and recovered files. The layout below was kept consistent for every step of the investigation.

```
C:\Forensics\Week10\
  Mantooth_Investigation\          (Autopsy case directory)
  EventLogs\                       (extracted Security.evtx)
    Parsed\                        (EvtxECmd CSV output)
  LNK\                             (extracted Recent\*.lnk files)
    Exports\                       (LECmd CSV output)
  Prefetch\                        (extracted XCOPY.EXE-*.pf)
  Registry\                        (extracted SYSTEM, SOFTWARE, SAM, SECURITY,
NTUSER.DAT)
  Recovered\                       (carved JPEGs, recovered files)
  Spool\                           (extracted .SPL / .SHD)
  Thumbcache\                      (extracted thumbcache_*.db)
```

Phase 1 — Case Creation and Evidence Ingestion

Step 1: Create the Autopsy Case

Autopsy 4.21 was launched and File → New Case opened the Case Information wizard. The Case Name was set to Mantooth_Investigation, the Base Directory was set to C:\Forensics\Week10\, and the Case Type was kept as Single-User. Autopsy uses these values to compute the final case directory C:\Forensics\Week10\Mantooth_Investigation, which is shown directly under the Base Directory field.

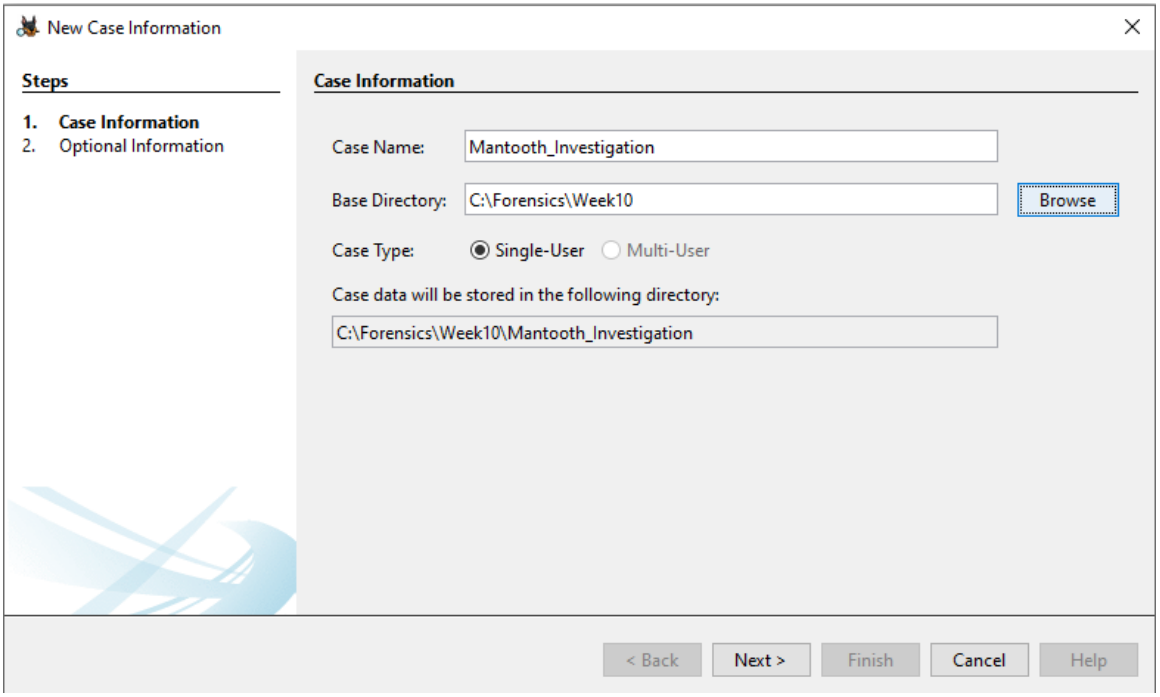


Fig 10.1 — Autopsy New Case Information dialog. Case Name: Mantooth_Investigation, Base Directory: C:\Forensics\Week10, Case Type: Single-User. Computed case path: C:\Forensics\Week10\Mantooth_Investigation.

Step 2: Optional Case Metadata

On clicking Next, the Optional Information page was completed with the case number, examiner identity, organisation name, and free-text notes describing the engagement. These fields are written into the Autopsy case database and surface again in the report header when Generate Report is run at the end of the week.

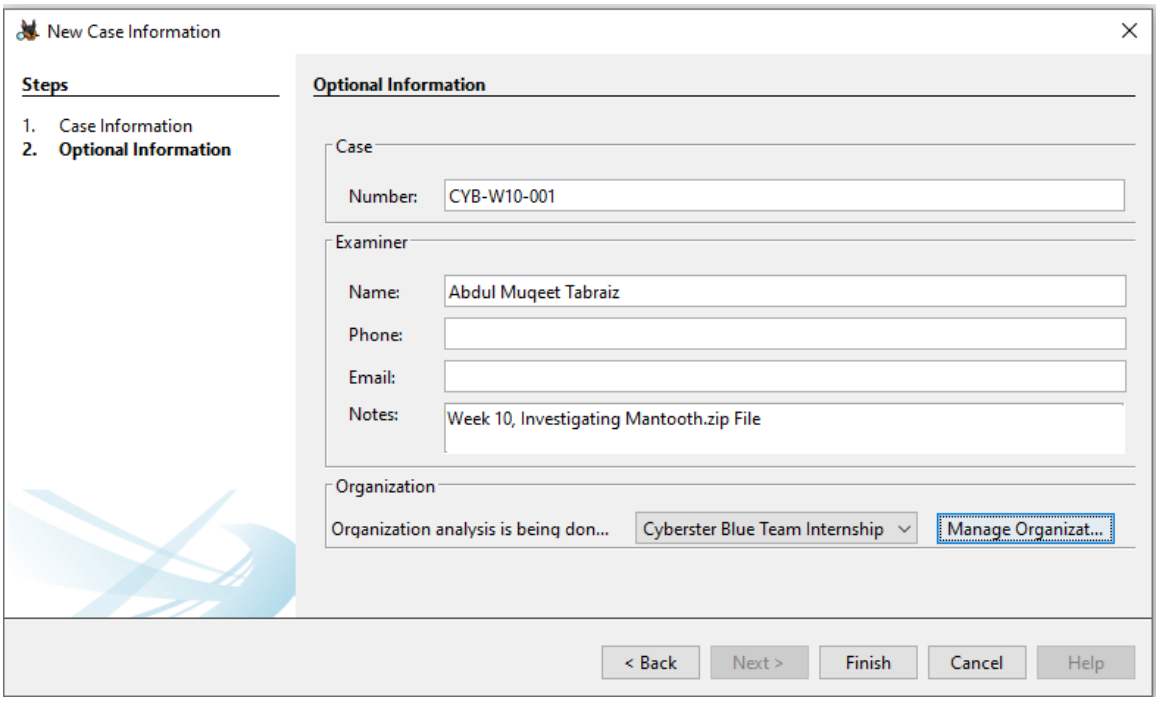


Fig 10.2 — Autopsy Optional Information page. Case Number: CYB-W10-001, Examiner: Abdul Muqeet Tabraiz, Organisation: Cyberster Blue Team Internship, Notes: "Week 10, Investigating Mantooth.zip File".

Step 3: Select the Data Source Type

Clicking Finish completed the case creation and the Add Data Source wizard launched automatically. Disk Image or VM File was selected because Mantooth.E01 is an Expert Witness (E01) disk image and Autopsy treats E01 / RAW / VMDK / VHD images through the same code path.

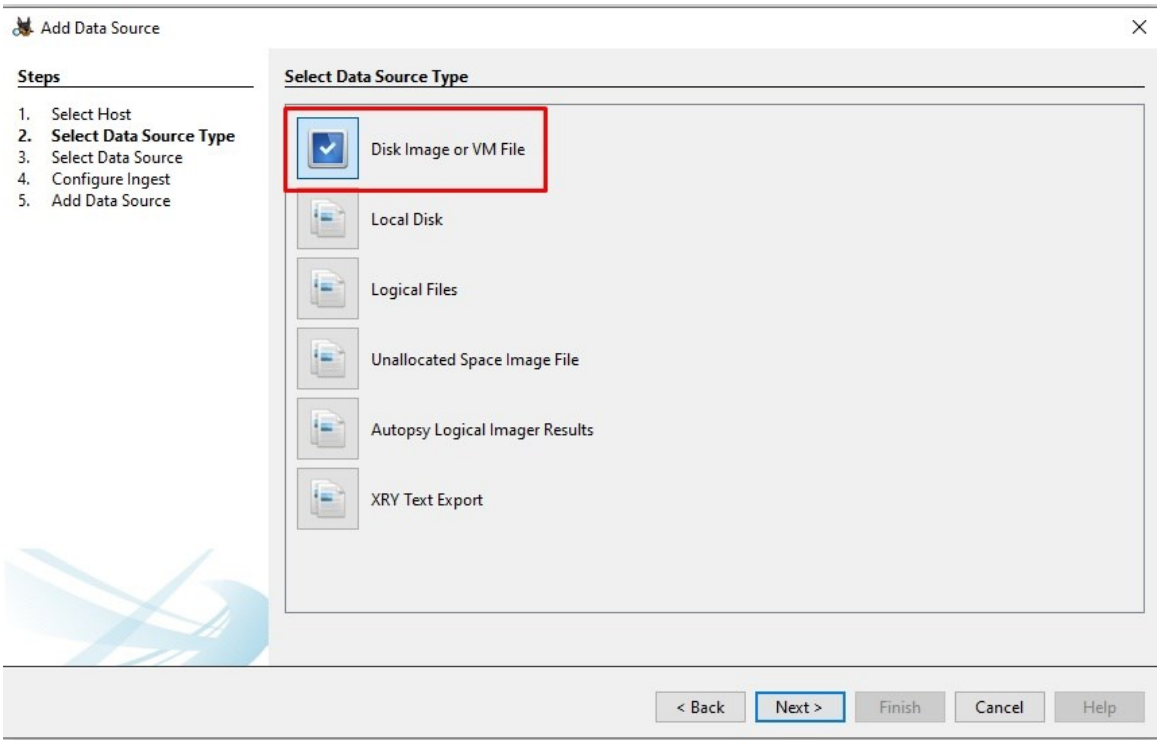


Fig 10.3 — Add Data Source wizard, step 2 of 5. Disk Image or VM File selected as the data source type for Mantooth.E01.

Step 4: Provide the Image Path AND Set the Time Zone (CRITICAL)

The Path field was browsed to C:\Forensics\Week10\Mantooth.E01. Critically, BEFORE clicking Next, the Time Zone dropdown was changed from the default UTC to (GMT-7:00) America/Denver (Mountain Time). This is the most operationally important checkbox in the entire workflow: the Mantooth machine resides in the Mountain Time zone, and applying any other timezone causes every Autopsy timestamp in the report to be displayed at the wrong wall-clock time. Sector size was left on Auto Detect.

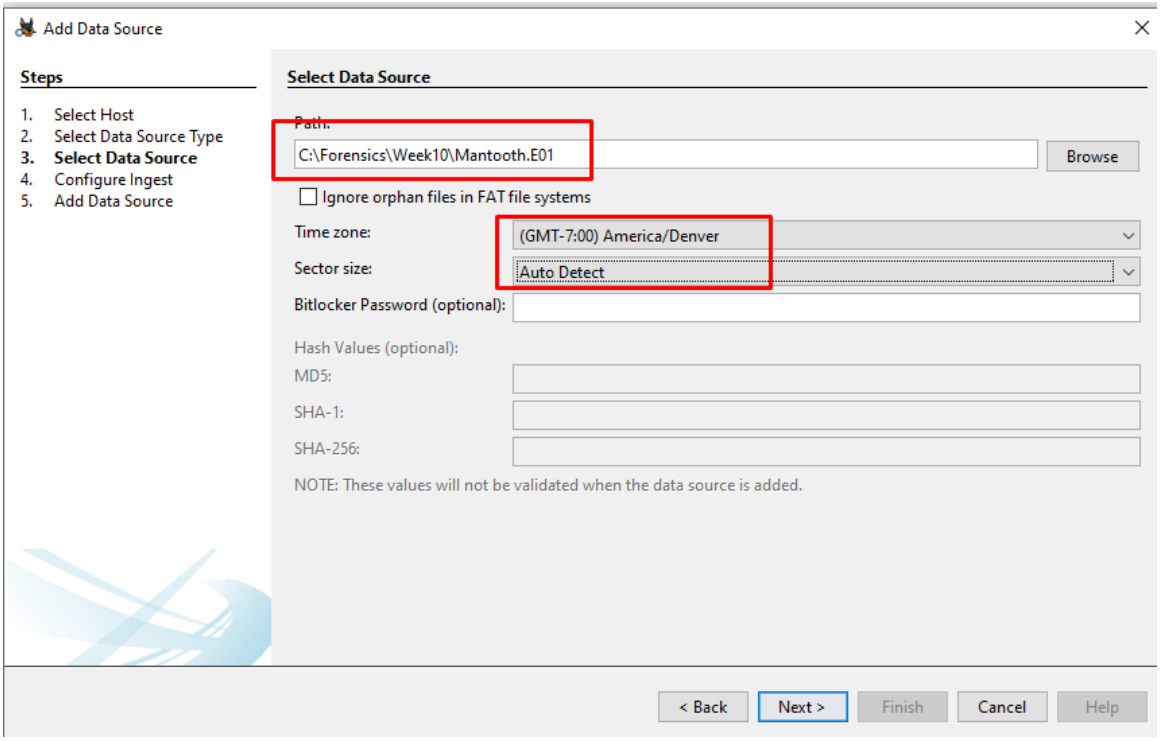


Fig 10.4 — Add Data Source wizard, step 3 of 5. Path: C:\Forensics\Week10\Mantooth.E01. Time zone set to (GMT-7:00) America/Denver — Mountain Time. Sector size: Auto Detect. Both red-boxed fields confirmed BEFORE clicking Next.

Step 5: Configure Ingest Modules

Run ingest modules on was set to All Files, Directories, and Unallocated Space — unallocated space is essential because Camerashy.exe was later recovered from a $Recycle.Bin entry and HARDCORE.jpg / pfah603.jpg were located in deleted/slack space. The following ingest modules were enabled:

- Recent Activity — populates Web History, Web Search, Web Cookies, Run Programs, USB Devices
- Hash Lookup — flags known files (used for the file-quality triage but not a primary deliverable for Q1)
- File Type Identification — drives Extension Mismatch and Picture Analyzer downstream
- Extension Mismatch Detector — surfaces files whose container header does not match their extension (anti-forensics indicator)
- Embedded File Extractor — unpacks zip / 7z / archive content so Email Parser can index .eml inside .pst etc.

- Picture Analyzer — runs EXIF extraction on JPEG / TIFF / RAW formats (drives Q3 Olympus answer)
- Keyword Search — built-in lists plus a custom Mantooth Investigation list (mantooth, check, cheque, ATM, fraud, TrueCrypt, VNC, camera, accomplice)
- Email Parser — parses .pst / .eml / .mbox to surface email addresses for Q7
- Interesting Files Identifier — built-in suspicious filename / path rules
- PhotoRec Carver — file carver against unallocated space (recovers deleted JPEGs)

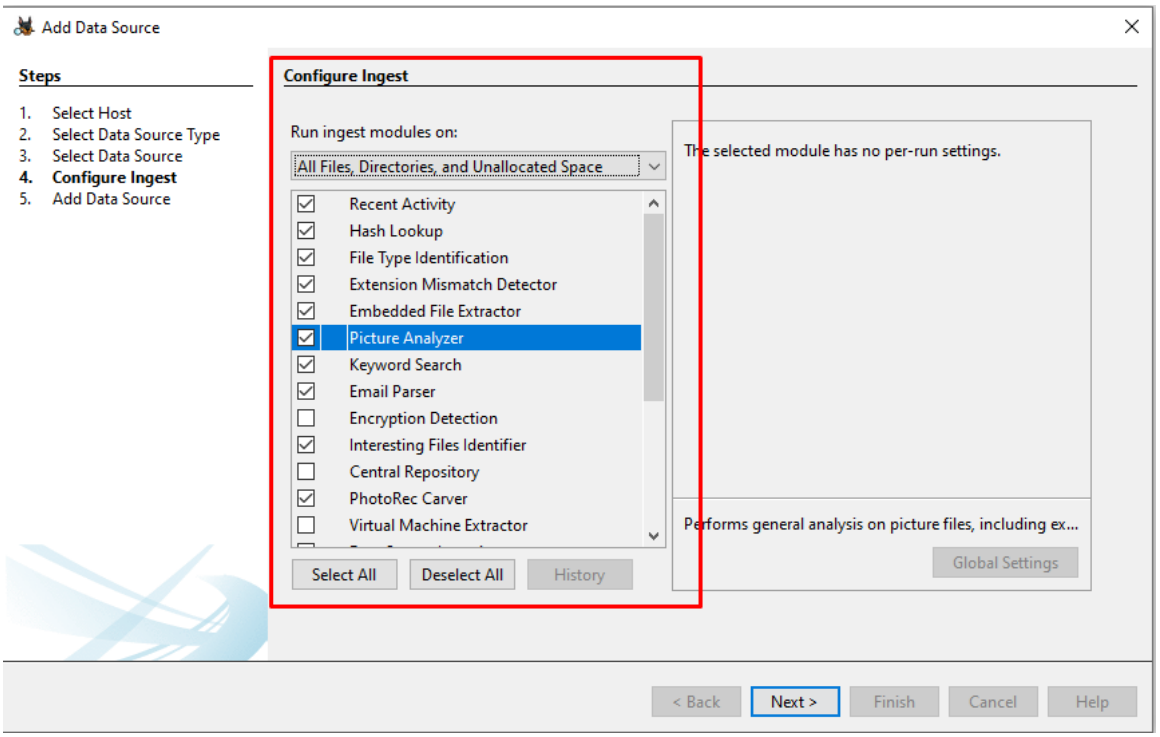


Fig 10.5 — Autopsy Configure Ingest screen. Run ingest modules on: All Files, Directories, and Unallocated Space. Ten modules enabled including Recent Activity, Hash Lookup, Picture Analyzer, Keyword Search, Email Parser, and Interesting Files Identifier.

On clicking Next and then Finish the data source was added and ingest started. Autopsy was left running uninterrupted for approximately three hours while the modules swept the 4-volume image. The progress indicator at the bottom-right was monitored but no other action was taken on the case until ingest fully completed.

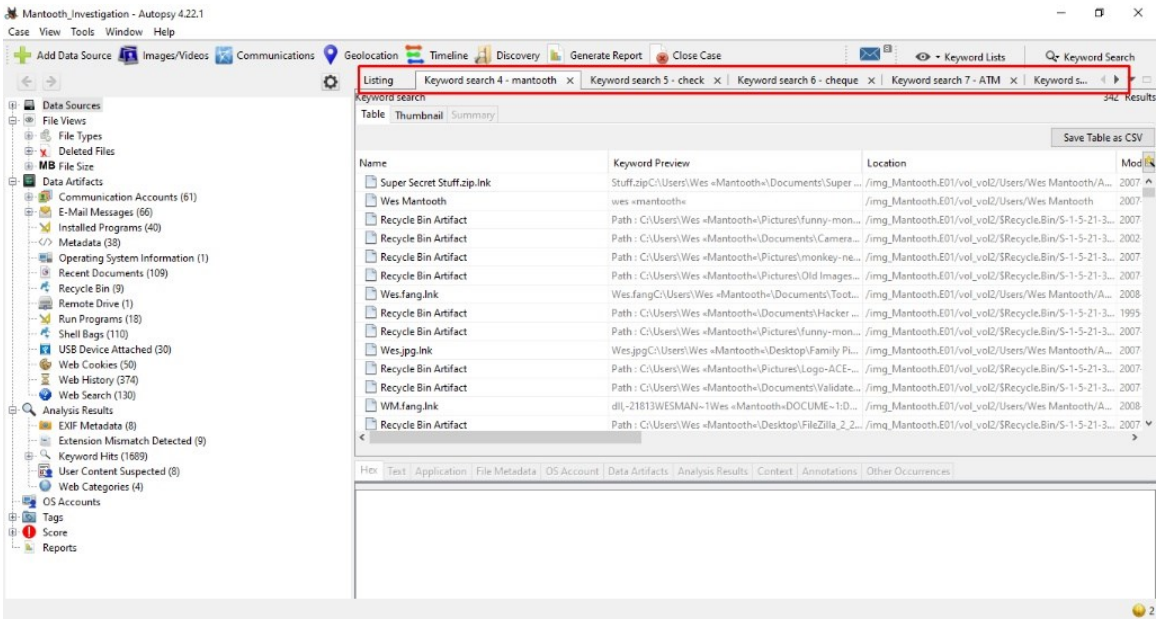


Fig 10.6 — Autopsy main window after ingest. Left panel populated with Data Sources, File Views, Deleted Files, Data Artifacts (Communication Accounts: 61, E-Mail Messages: 66, Installed Programs: 40, Metadata: 38, Recent Documents: 109, Recycle Bin: 9, Run Programs: 18, Shell Bags: 110, USB Device Attached: 30, Web Cookies: 50, Web History: 374, Web Search: 130), and Analysis Results (EXIF Metadata: 8, Extension Mismatch: 9, Keyword Hits: 1689, User Content Suspected: 8, Web Categories: 4). Open keyword search tabs visible: mantooth, check, cheque, ATM.

Phase 2 — Image Verification (Q1 — MD5 Hash)

Step 1: Read the Data Source Integrity Result

After ingest completed, the Data Source Integrity Module result was opened by selecting the Mantooth.E01 data source in the left panel and reviewing the verification panel. Autopsy reported Result: verified, MD5 hash verified, with the Calculated hash matching the Stored hash that is embedded in the E01 container.

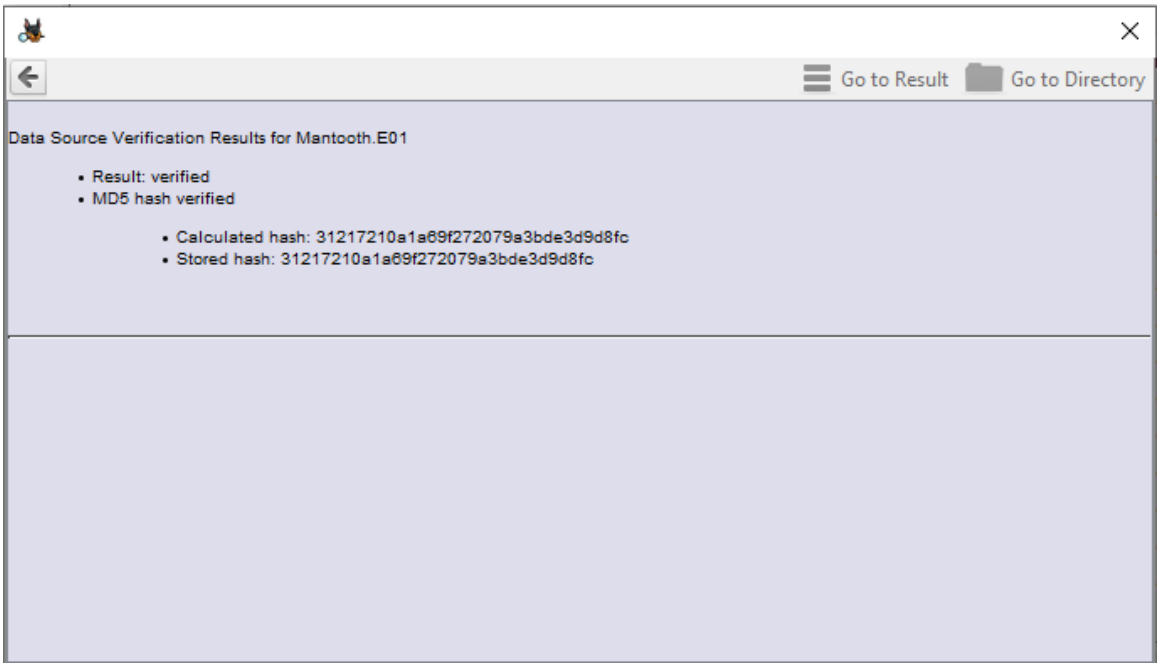


Fig 10.7 — Autopsy Data Source Verification Results for Mantooth.E01. Result: verified. MD5 hash verified — Calculated: 31217210a1a69f272079a3bde3d9d8fc, Stored: 31217210a1a69f272079a3bde3d9d8fc. Q1 PRIMARY DELIVERABLE.

Q1 Answer Summary

Metric	Value
Image filename	Mantooth.E01
Hash algorithm	MD5
Calculated hash	31217210a1a69f272079a3bde3d9d8fc
Stored (embedded) hash	31217210a1a69f272079a3bde3d9d8fc
Verification result	VERIFIED — match
Verification method	Autopsy Data Source Integrity ingest module

Phase 3 — Partition Structure Analysis (Q2)

Mantooth.E01 was expanded in the Autopsy left-panel tree. Selecting each volume populated the bottom panel with file-system type, starting sector and length-in-sectors. The image contains four volumes: a small unallocated boot region, the primary NTFS / exFAT Windows partition, a small DOS FAT12 utility partition, and a trailing unallocated region.

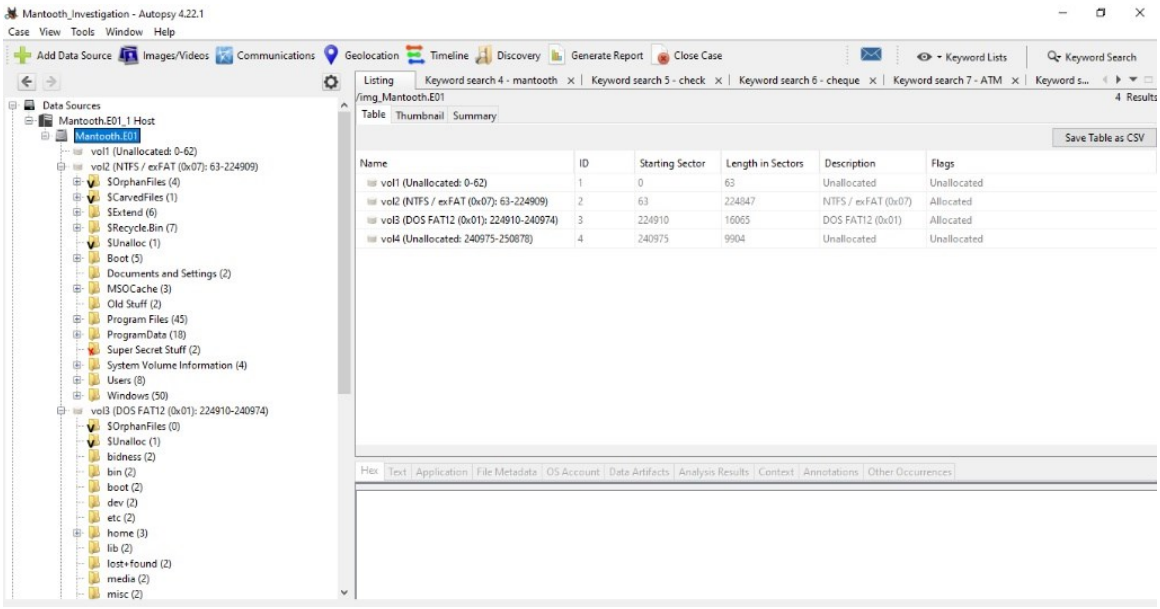


Fig 10.8 — Autopsy partition view of /img_Mantooth.E01. Four volumes: vol1 Unallocated (0–62), vol2 NTFS/exFAT (0x07) starting sector 63 length 224847, vol3 DOS FAT12 (0x01) starting sector 224910 length 16065 (Allocated), vol4 Unallocated (240975 length 9904). Q2 PRIMARY DELIVERABLE — vol2 holds the Windows installation, vol3 is the DOS utility partition.

Volume	Start Sector	Length (Sectors)	File System	Description / Contents
vol1	0	63	Unallocated	Pre-partition boot/MBR region
vol2	63	224847	NTFS / exFAT (0x07)	Primary Windows partition — Users\Wes Mantooth, Program Files, Windows\System32, $Recycle.Bin, $MFT — main evidence volume
vol3	224910	16065	DOS FAT12 (0x01)	Small utility partition with bin / boot / dev / home / lib / etc — possible recovery or Linux toolset
vol4	240975	9904	Unallocated	Trailing unallocated space (carving target)

Phase 4 — EXIF Metadata and Olympus Photo (Q3)

Results → Extracted Content → EXIF Metadata returned eight image entries. The Device Make column was sorted to surface the OLYMPUS OPTICAL CO.,LTD entry. Selecting that row loaded the Application tab, which rendered the JPEG: a high-end speedboat sitting on a trailer in a workshop. The investigative significance is twofold — it ties Mantooth to an Olympus C730UZ camera (which also appears in the USB device list in Part B Q11/Q12), and the photo location lives under /img_Mantooth.E01/vol_vol3/Stuff/, a non-standard directory on the small DOS FAT12 partition that does not appear on the main Windows partition.

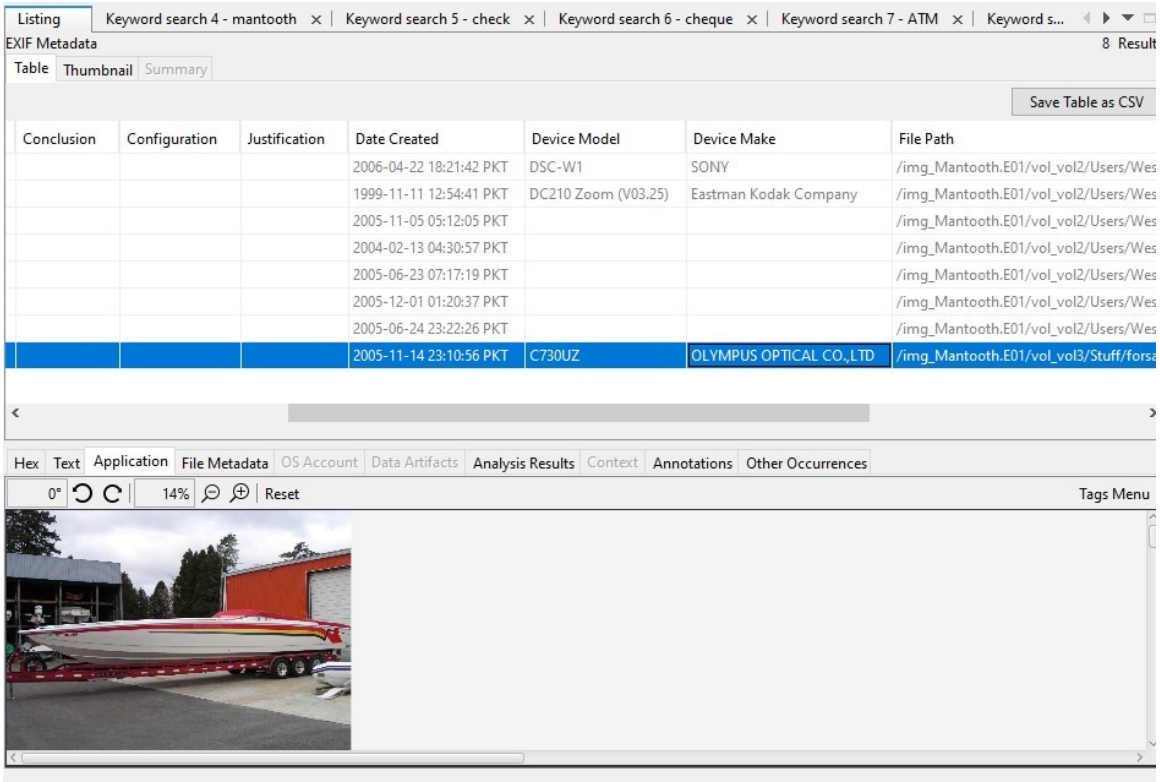


Fig 10.9 — Autopsy EXIF Metadata results, eight rows. Highlighted row — Date Created: 2005-11-14 23:10:56 PKT, Device Model: C730UZ, Device Make: OLYMPUS OPTICAL CO.,LTD. File path: /img_Mantooth.E01/vol_vol3/Stuff/forsa[le boat]. Q3 PRIMARY DELIVERABLE.

The matching JPEG was right-clicked and tagged as Q3 - Olympus Photo so the bookmark would survive into the final Generate Report output.

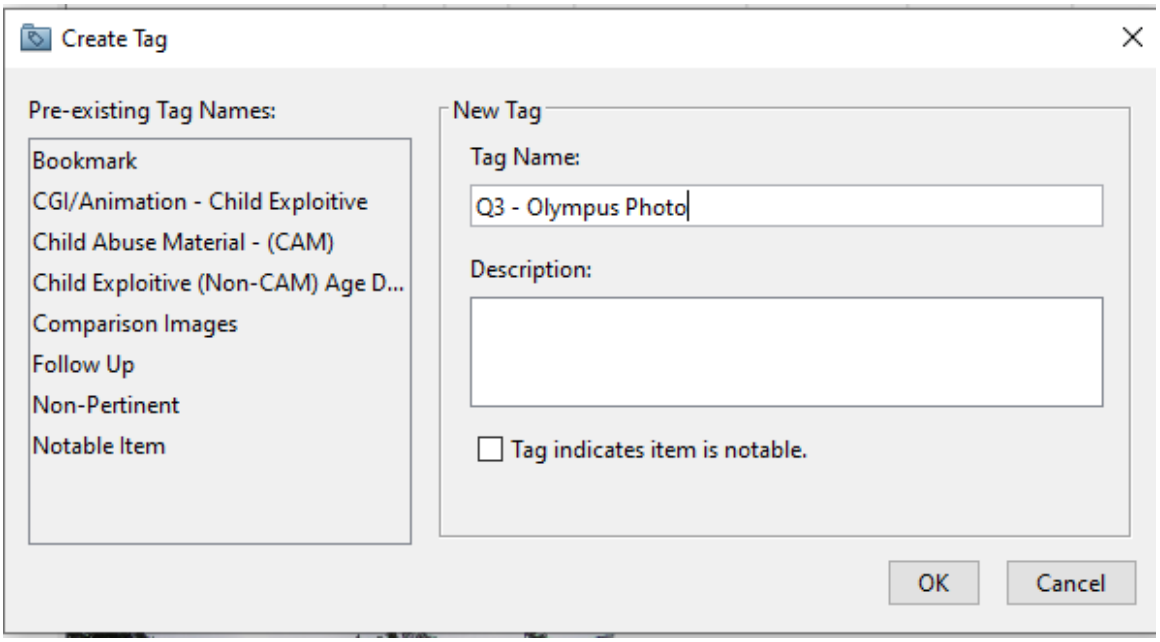


Fig 10.10 — Autopsy Create Tag dialog. Tag Name: "Q3 - Olympus Photo". Pre-existing tag names visible (Bookmark, Notable Item, Follow Up, Comparison Images).

Field	Value
Camera make	OLYMPUS OPTICAL CO.,LTD
Camera model	C730UZ
Date created (EXIF)	2005-11-14 23:10:56 PKT
File path	/img_Mantooth.E01/vol_vol3/Stuff/<boat-for-sale>.jpg
Volume	vol3 (DOS FAT12 utility partition)
Tag applied	Q3 - Olympus Photo

Phase 5 — Encrypted Document Discovery (Q4)

The Interesting Files Identifier flagged an encrypted Microsoft Word document inside a Windows Mail Inbox EML attachment. Navigating /img_Mantooth.E01/vol_vol2/Users/Wes Mantooth/AppData/Local/Microsoft/Windows Mail/Local Folders/Inbox/61A02D20-0000000F.eml/ exposed a child file named "How To Steal Credit Numbers.doc" — a 27,648-byte application/msword file rendered by Autopsy as Encrypted Document. All four MAC timestamps display 0000-00-00 00:00:00, a telltale of EML attachment metadata stripping. The filename alone ("How To Steal Credit Numbers.doc") together with the encrypted payload makes this a Notable Item for the case.

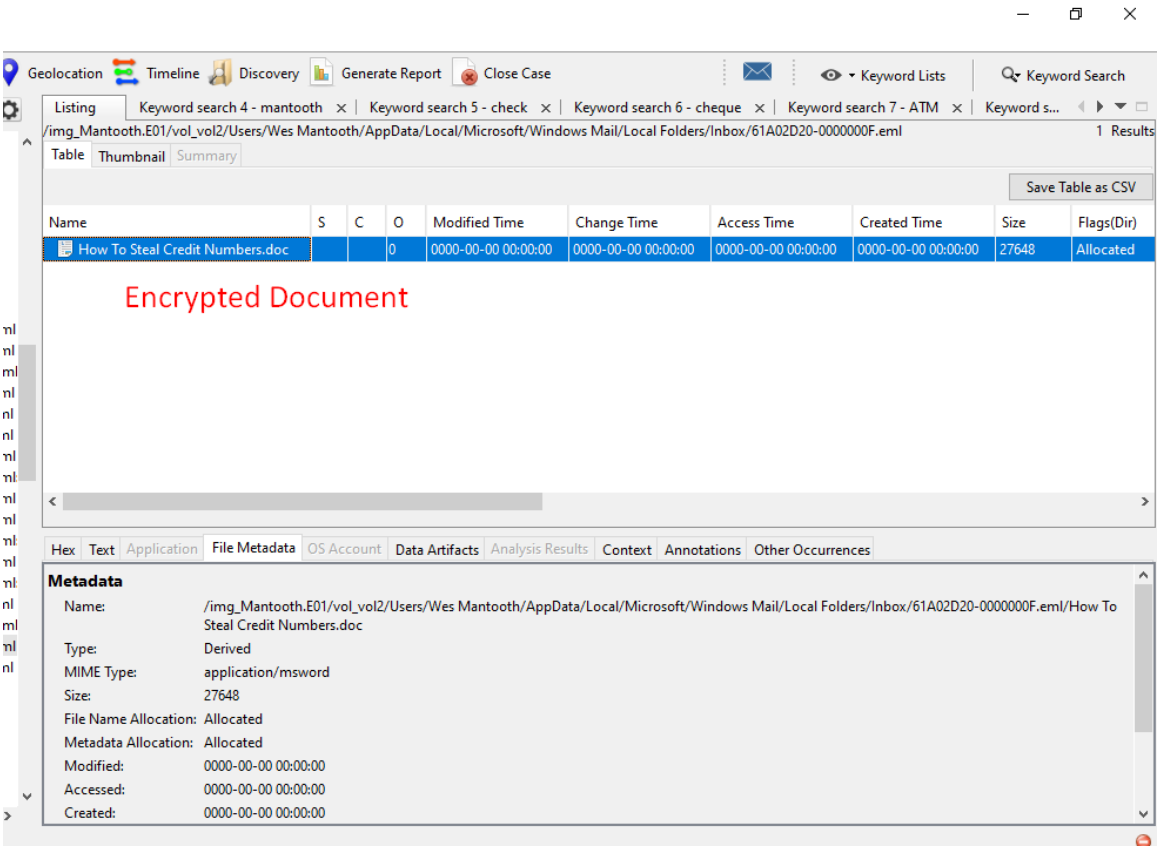


Fig 10.11 — Autopsy file metadata view for How To Steal Credit Numbers.doc. Type: Derived. MIME Type: application/msword. Size: 27648. File Name Allocation: Allocated. Modified / Accessed / Created: 0000-00-00 00:00:00. Annotated as "Encrypted Document". Q4 PRIMARY DELIVERABLE.

Field	Value
File name	How To Steal Credit Numbers.doc
Container	61A02D20-0000000F.eml (Windows Mail Inbox)
Path	/img_Mantooth.E01/vol_vol2/Users/Wes Mantooth/AppData/Local/Microsoft/Windows Mail/Local Folders/Inbox/
Size	27,648 bytes

MIME Type	application/msword
Encryption indicator	Autopsy banner "Encrypted Document"; null timestamps
Investigative note	Filename references credit card theft; encrypted payload deliberately blocks examination

Phase 6 — Deleted Files: HARDCORE.jpg and pfah603.jpg (Q5)

Step 1: Locating HARDCORE.jpg

Tools → Keyword Search → search term HARDCORE returned five matching keyword hits. The primary hit was "My poem.txt:HARDCORE.JPG" — an Alternate Data Stream attached to My poem.txt under /img_Mantooth.E01/vol_vol2/Users/Wes Mantooth/Documents/. The file is 58,348 bytes, MIME image/jpeg, Allocated in both file-name and metadata, with MAC timestamps Modified 2007-04-13 06:06:14, Accessed 2007-07-13 23:37:44, Created 2007-04-13 06:01:38, Changed 2007-09-27 18:10:45. MD5 e16ffc19575863c840e4f5f1b18cbd6 and SHA-256 45c30206ffad970850f7fbefdc7288773d315b0082388c918a6536882d5fd90f computed by Autopsy.

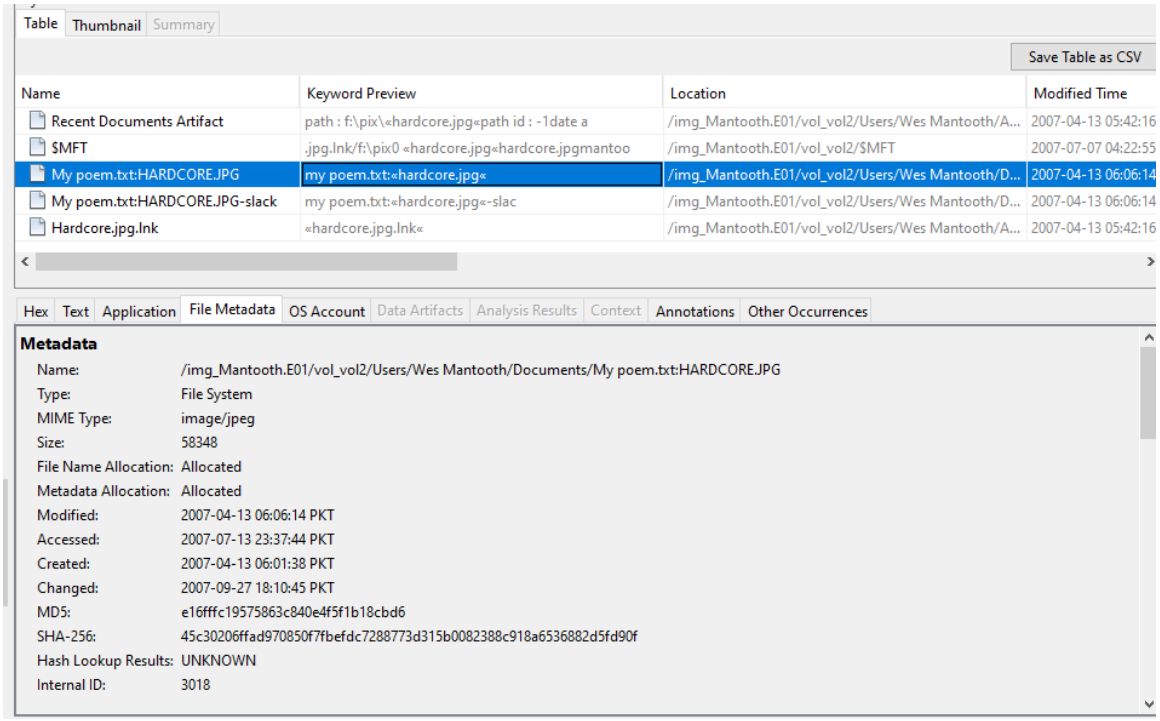


Fig 10.12 — Autopsy keyword search hit for HARDCORE. Selected entry: My poem.txt:HARDCORE.JPG at /img_Mantooth.E01/vol_vol2/Users/Wes Mantooth/Documents/. Size 58348, MIME image/jpeg, MD5 e16ffc19575863c840e4f5f1b18cbd6, Hash Lookup: UNKNOWN. Q5 ANSWER PART 1.

The hidden JPEG was extracted via right-click → Extract File and saved into C:\Forensics\Week10\Recovered\My poem.txt_HARDCORE.JPG.

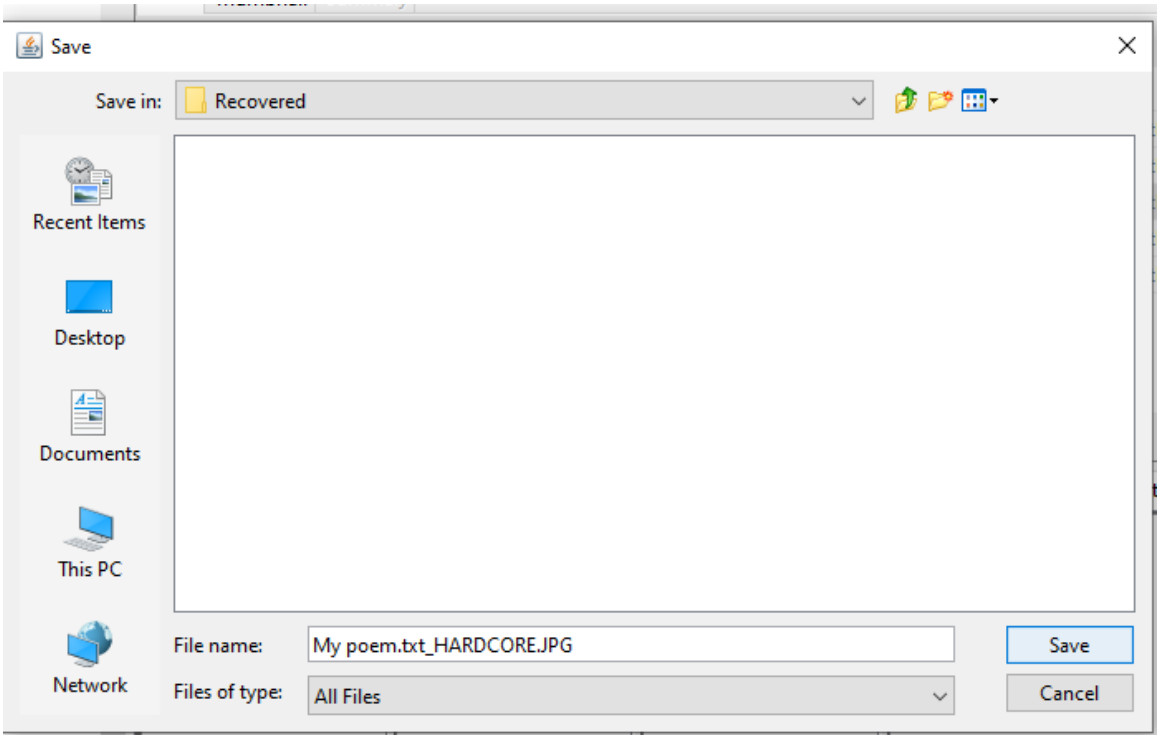


Fig 10.13 — Autopsy Save dialog. File name: My poem.txt_HARDCORE.JPG, target folder Recovered. JPEG carved out of the ADS for visual inspection.

Investigative note — the JPEG is concealed inside an Alternate Data Stream attached to My poem.txt. NTFS ADS is a classic Windows hiding technique because the host file (My poem.txt) appears innocuous in Explorer, the stream content does not show in directory listings without /R, and dir size reports the host size only. The Hash Lookup result of UNKNOWN means the JPEG content is not in any of the loaded NSRL hash sets, so it is a user-supplied or modified image rather than a stock OS file.

Step 2: Locating pfah603.jpg

A second keyword search for pfah603 returned three matches. The primary hit was "readthis.txt:pfah603.jpg" — another ADS, this time attached to readthis.txt under /img_Mantooth.E01/vol_vol2/Users/Wes Mantooth/Documents/ADS/. The pfah603 stream is 53,763 bytes, MIME image/jpeg, Allocated. MAC timestamps Modified 2007-07-13 23:59:08, Accessed 2007-07-14 00:05:02, Created 2007-03-06 07:16:55, Changed 2007-09-27 18:10:44. MD5 45211e60c4e02e64961dc242efaf28ba and SHA-256 43c2bee19c1c4b5da91080dbc384e6254e9a511a1e5bccbb32609de71459db38.

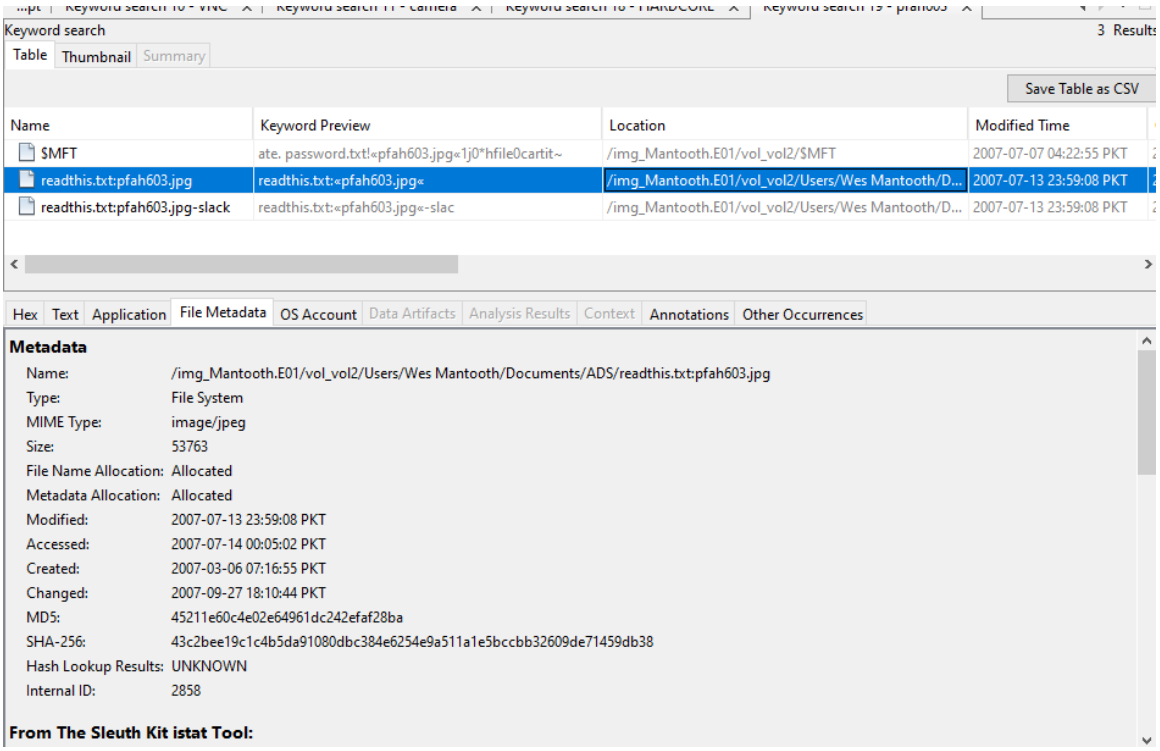


Fig 10.14 — Autopsy keyword search hit for pfah603. Selected entry: readthis.txt:pfah603.jpg at /img_Mantooth.E01/vol_vol2/Users/Wes Mantooth/Documents/ADS/. Size 53763, MIME image/jpeg, MD5 45211e60c4e02e64961dc242efaf28ba, Hash Lookup: UNKNOWN. Q5 ANSWER PART 2.

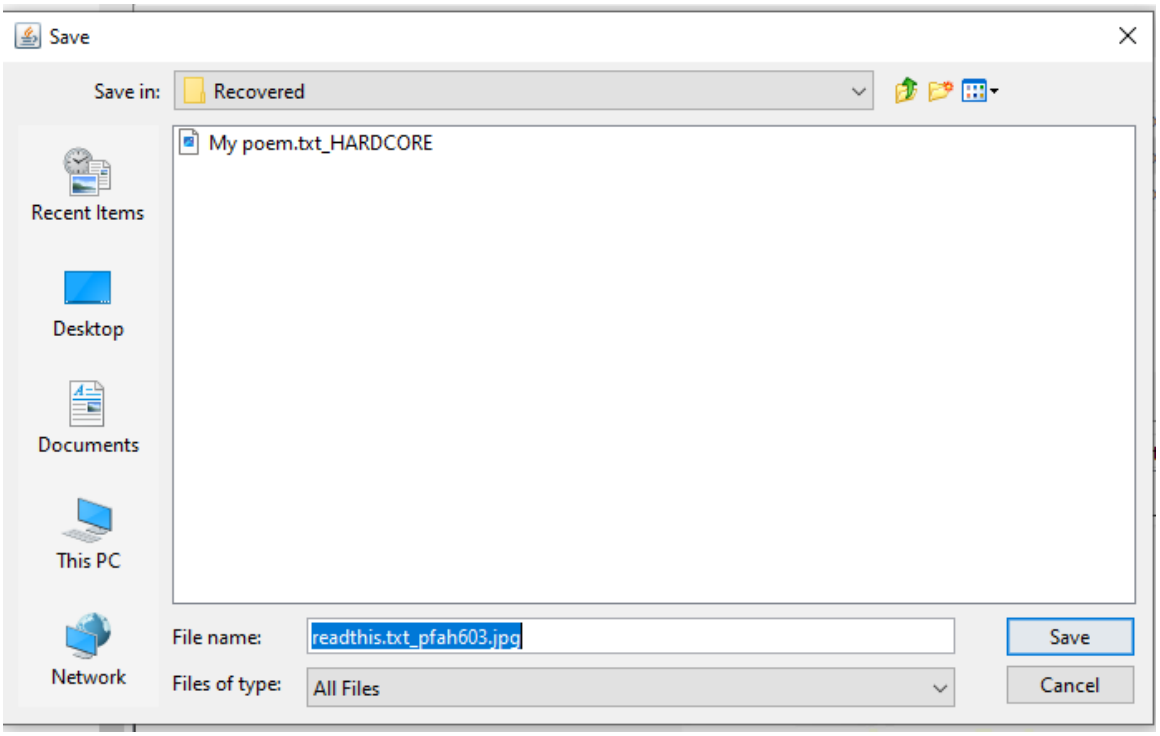


Fig 10.15 — Autopsy Save dialog with My poem.txt_HARDCORE already in the Recovered folder; readthis.txt_pfah603.jpg about to be added beside it.

Field	HARDCORE.jpg (ADS)	pfah603.jpg (ADS)
Host file	My poem.txt	readthis.txt

Host folder	Users\Wes Mantooth\Documents\	Users\Wes Mantooth\Documents\ADS\
Stream size	58,348 bytes	53,763 bytes
MIME	image/jpeg	image/jpeg
Allocation	Allocated	Allocated
Created	2007-04-13 06:01:38	2007-03-06 07:16:55
Modified	2007-04-13 06:06:14	2007-07-13 23:59:08
MD5	e16ffc19575863c840e4f5f1b18cbd6	45211e60c4e02e64961dc242efaf28ba
Recovered to	Recovered\My poem.txt_HARDCORE.JPG	Recovered\readthis.txt_pfah603.jpg

The deliberate choice of placing the second JPEG inside a folder literally named ADS is operationally telling — Mantooth knew exactly what an Alternate Data Stream was and named the parent folder accordingly. Both JPEGs are flagged as candidates for Camerashy.exe steganography processing in Part C.

Phase 7 — Web Search History Analysis (Q6)

Results → Extracted Content → Web Search returned 130 search-query rows. Sorting by Date Accessed descending placed the most recent queries at the top, all sourced from index.dat (Internet Explorer Analyzer parser) under /img_Mantooth.E01/vol_vol2/Users/Wes Mantooth/AppData/Local/Microsoft/Windows/Temporary Internet Files/. The dominant search domain is google.com. Three investigative themes stand out — methamphetamine production ("making meth"), check-fraud techniques ("check washing"), and ATM fraud ("atm card stealing").

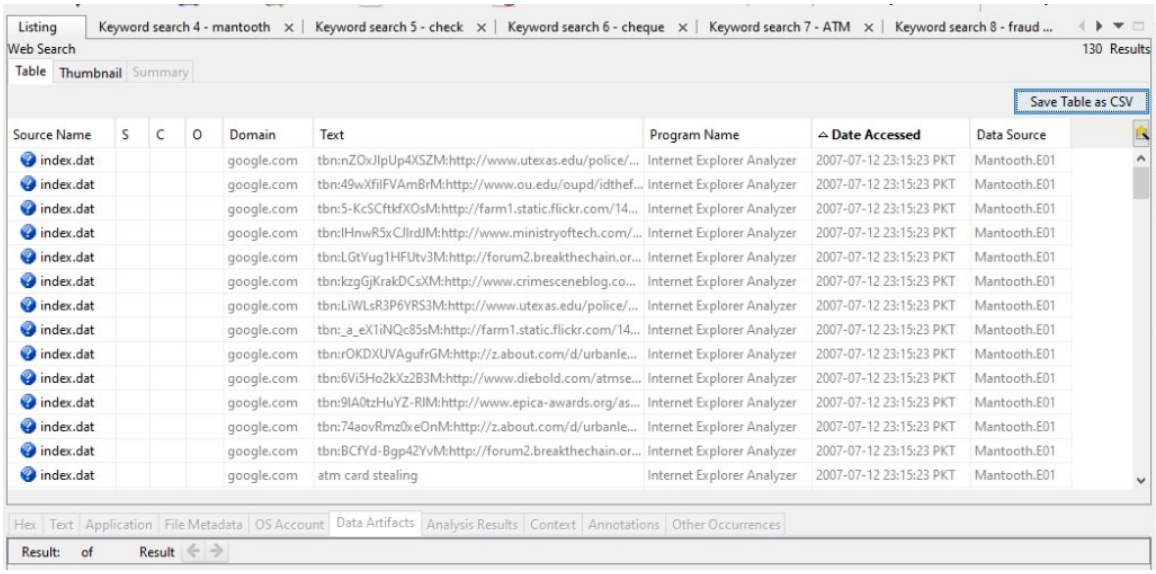


Fig 10.16 — Autopsy Web Search results panel, 130 rows. Selected sample: tbn:nZOxJlpUp4XSZM:http://www.utexas.edu/police/, Domain google.com, Program Internet Explorer Analyzer, Date Accessed 2007-07-12 23:15:23 PKT, Data Source Mantooth.E01. Visible plain-text query rows include atm card stealing, check washing, making meth, diebold/atmse, urbanle, breakthechain. Q6 PRIMARY DELIVERABLE.

Search Topic	Sample Query Strings	Browser	Date Range (PKT)	Why Significant
ATM fraud	"atm card stealing" (multiple hits)	Internet Explorer	2007-07-12 23:15:24 — 23:17:30	Direct intent to commit ATM card theft
Check fraud	"check washing" (multiple hits)	Internet Explorer	2007-07-12 23:17:30 — 23:17:36	Methodology research for the cheque-fraud case

Drug manufacture	"making meth" (multiple hits)	Internet Explorer	2007-07-12 23:16:33 — 23:17:08	Adjacent illegal-conduct research; relevant to overall criminality assessment
Reference / how-to	diebold atmse, urbanlegends, breakthechain	Internet Explorer	2007-07-12 23:15:23 — 23:17:42	Supporting domains showing follow-on browsing tied to the three queries above

Phase 8 — IP Address and Email Address Extraction (Q7)

Step 1: IP Address Sweep with Keyword Lists

Autopsy's built-in IP Addresses keyword list returned 245 unique IP entries across the image. Sorting Files With Hits descending highlighted the IPs that appeared most frequently — a useful proxy for which addresses were repeatedly contacted (mail servers, advertising trackers, command-and-control candidates) versus one-off references.

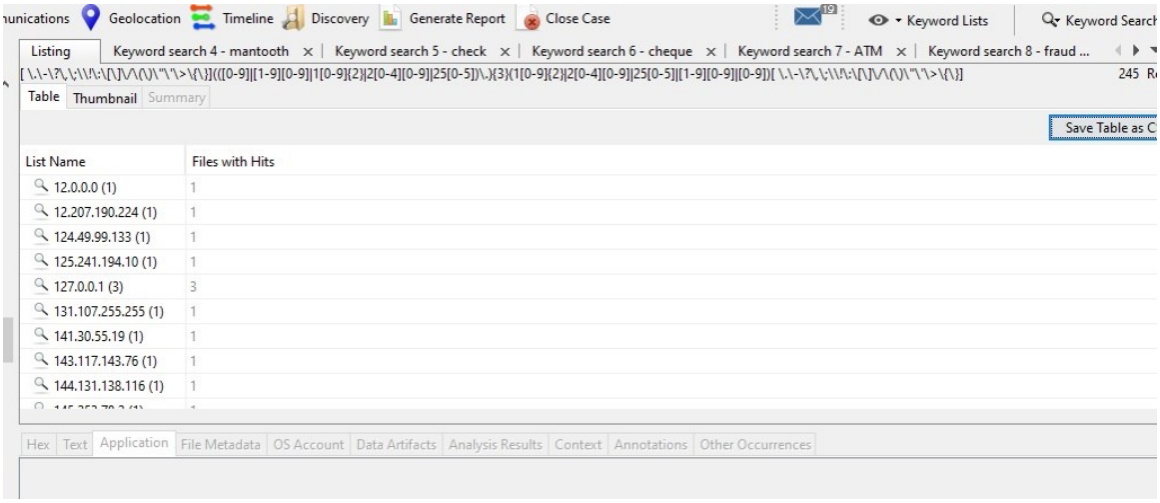
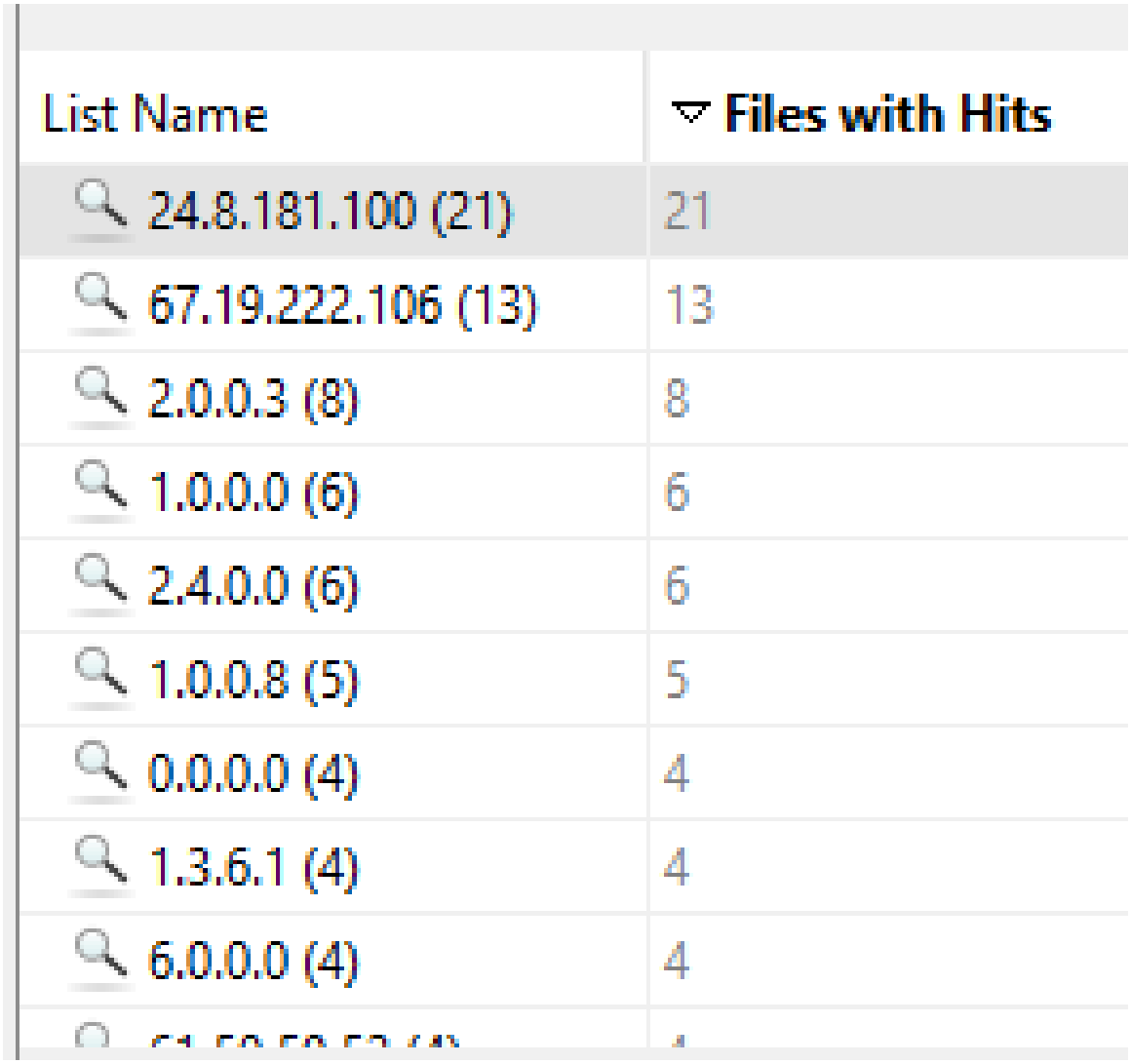


Fig 10.17 — Autopsy IP Addresses keyword list result, 245 rows. Sample entries 12.0.0.0, 12.207.190.224, 124.49.99.133, 125.241.194.10, 127.0.0.1 (3 hits), 131.107.255.255, 141.30.55.19, 143.117.143.76, 144.131.138.116. Q7 PART 1.



List Name	Files with Hits
24.8.181.100 (21)	21
67.19.222.106 (13)	13
2.0.0.3 (8)	8
1.0.0.0 (6)	6
2.4.0.0 (6)	6
1.0.0.8 (5)	5
0.0.0.0 (4)	4
1.3.6.1 (4)	4
6.0.0.0 (4)	4

Fig 10.18 — Top IP addresses sorted by Files With Hits. 24.8.181.100 — 21 hits, 67.19.222.106 — 13 hits, 2.0.0.3 — 8 hits, 1.0.0.0 — 6 hits, 2.4.0.0 — 6 hits, 1.0.0.8 — 5 hits, 0.0.0.0 — 4 hits, 1.3.6.1 — 4 hits, 6.0.0.0 — 4 hits.

The three top addresses were drilled down individually to identify their host context.

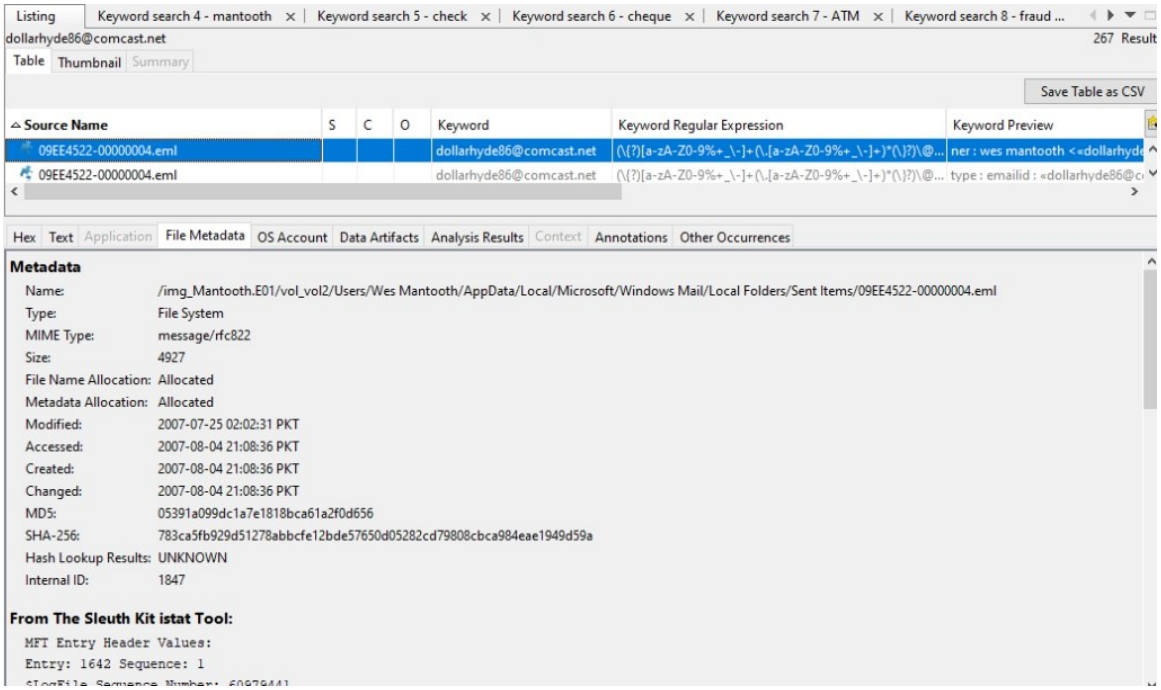


Fig 10.19 — 24.8.181.100, 21 hits. Sample sources: 0C130270-0000000D.eml, 40A511AF-00000008.eml, Outlook.pst. Keyword preview shows ".hsd1.co.comcast.net=24.8.181.100=" by comcast. Selected file metadata: /img_Mantooth.E01/vol_vol2/Users/Wes Mantooth/AppData/Local/Microsoft/Windows Mail/Local Folders/Inbox/0C130270-0000000D.eml, MIME message/rfc822, MD5 7fa7a8689fe7d645f5ff806be1051c2a. Confirms Comcast residential IP captured in Windows Mail email headers.

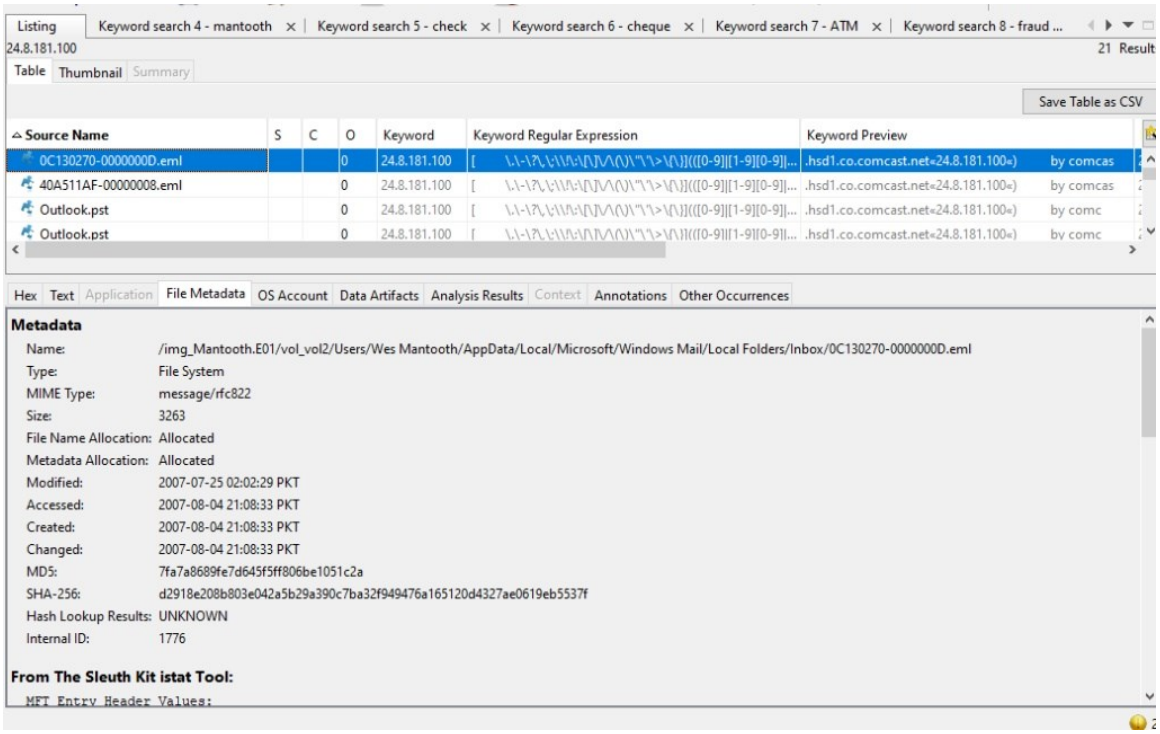


Fig 10.20 — 67.19.222.106, 13 hits. Sources are repeated index.dat hits at /img_Mantooth.E01/vol_vol2/Users/Wes Mantooth/AppData/Local/Microsoft/Windows/Temporary Internet Files/Low/Content.IE5/index.dat. Keyword preview: url:http://=67.19.222.106=crime/graphics/camer. Modified Time 2007-07-13 04:51:48 PKT. Direct browser hit on a remote crime-related URL.

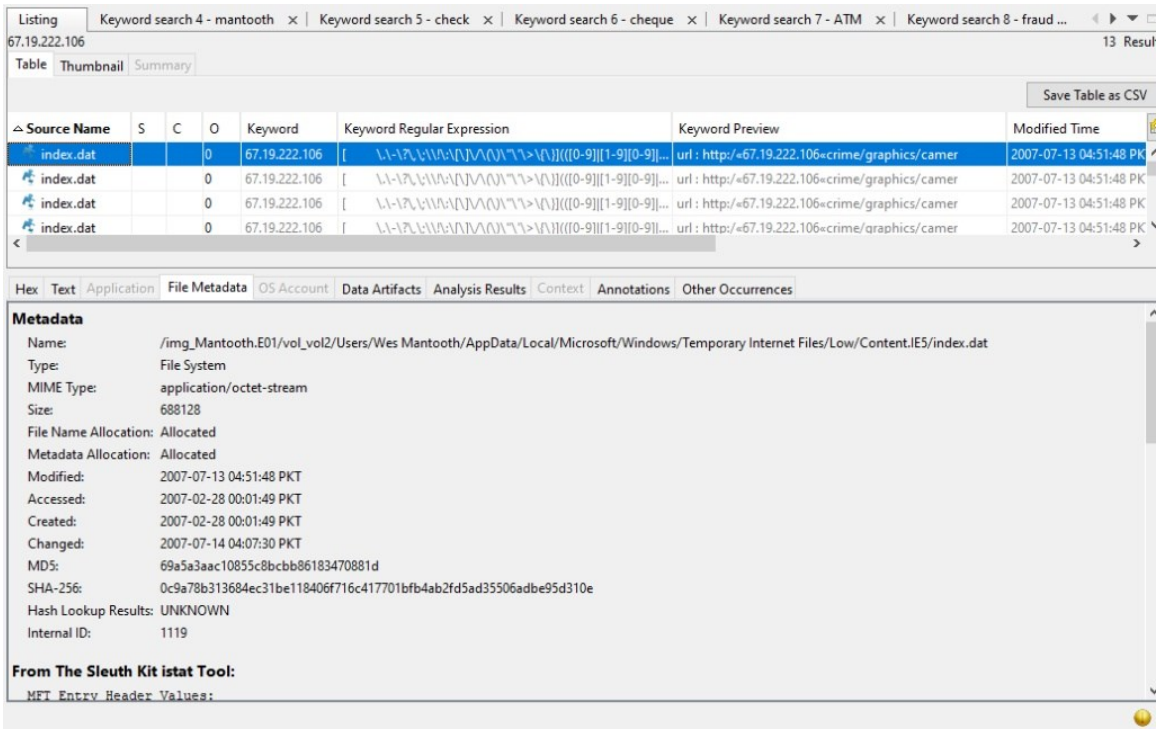


Fig 10.21 — 2.0.0.3, 8 hits. Sources include NTUSER.DAT and SOFTWARE registry hives. Keyword preview: "e:emozilla firefox =2.0.0.3=slowinfocachechang" and "e:mozilla firefox =2.0.0.3= v.2.0.0.3 (en-us)". This is not a network IP — it is a Firefox version string false-positive. Recorded for completeness.

IP	Hits	Source(s)	Investigative Context
24.8.181.100	21	Inbox EMLs, Outlook.pst	Comcast residential IP from Mantooth's incoming email headers
67.19.222.106	13	index.dat (IE Temp Files)	Browsed URL host — "crime/graphics/cameras" path; clearly investigative
2.0.0.3	8	NTUSER.DAT, SOFTWARE	False positive — Firefox 2.0.0.3 version string
127.0.0.1	3	Various	Localhost loopback — benign

Step 2: Email Address Sweep with Keyword Lists

The same approach was used for the built-in Email Addresses keyword list. The top hits below all map to Mantooth-owned mail accounts or to people he was corresponding with.

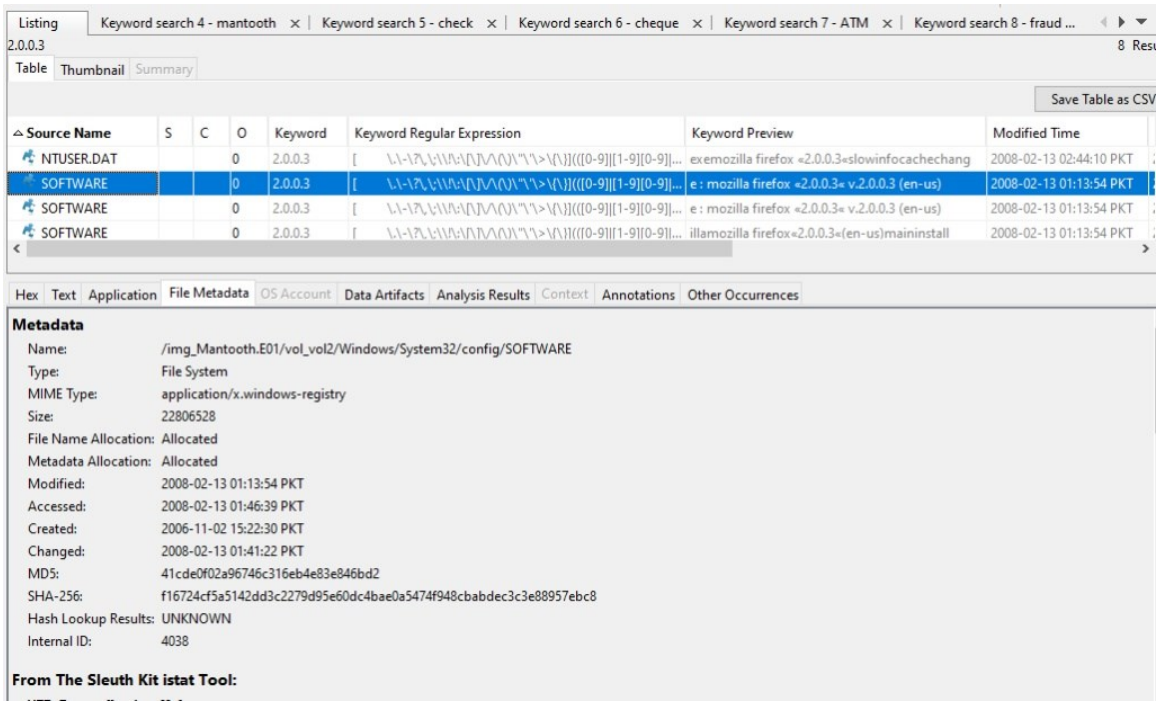


Fig 10.22 — Autopsy Email Addresses keyword list. dollarhyde86@comcast.net — 267 matches across 108 files (top result). chkwasher@comcast.net — 165 across 70 files. smee.rox@gmail.com — 88 across 39 files. txkidd@swbell.net — 89 across 38 files. toothfairy@mentaldental.com — 34 across 14 files. mail-noreply@google.com — 80 across 13 files. pgp_corporation_laura_lee@mail.vresp.com — 13 across 9 files. skimmerman27@hotmail.com — 21 across 9 files. Q7 PART 2.

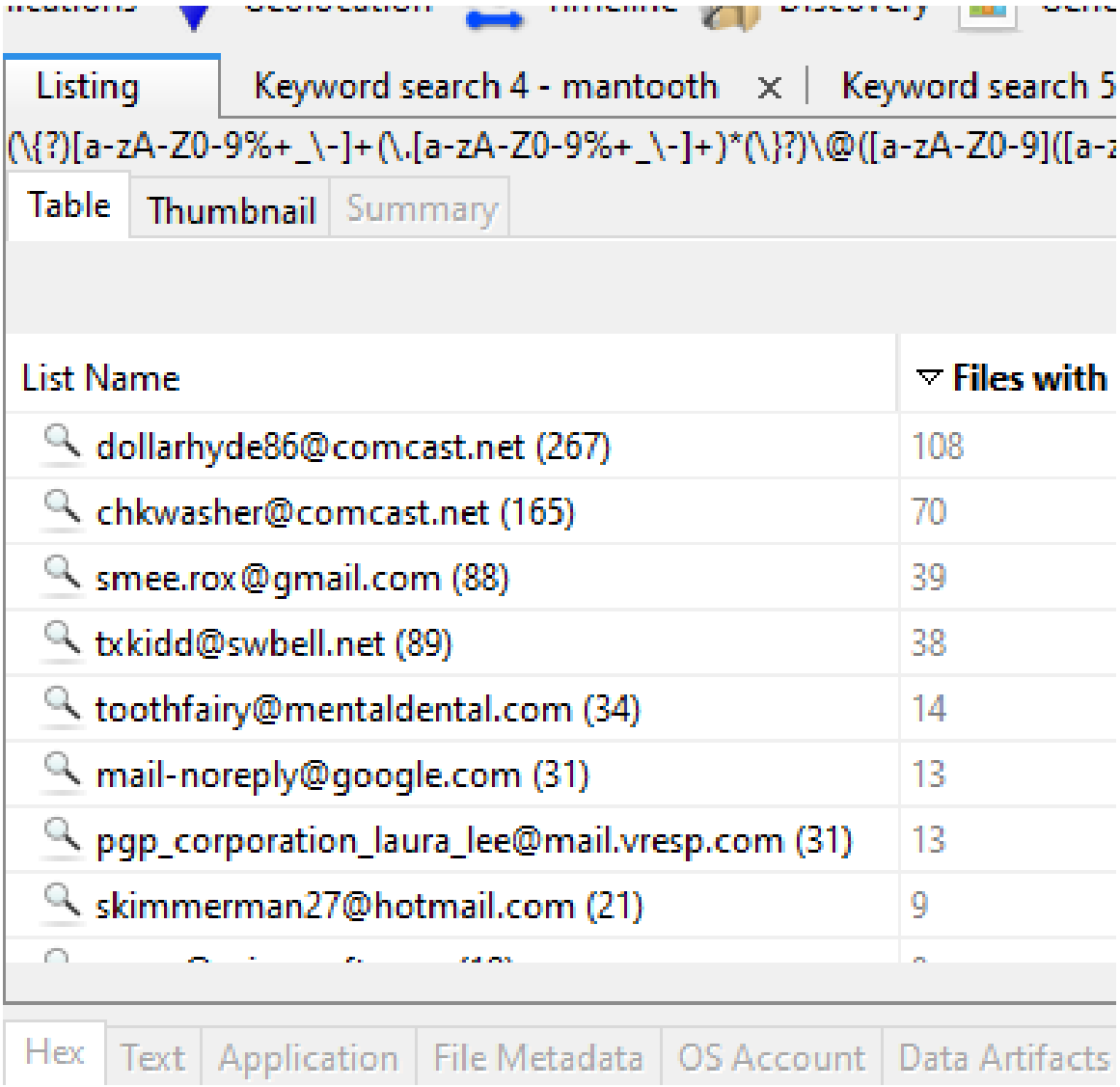


Fig 10.23 — dollarhyde86@comcast.net inside 09EE4522-00000004.eml (Sent Items). Keyword preview "ner: wes mantooth <<dollarhyd..." and "type: emailid: <<dollarhyde86@c...>>". Strongly suggests this is a Mantooth-owned outgoing identity.

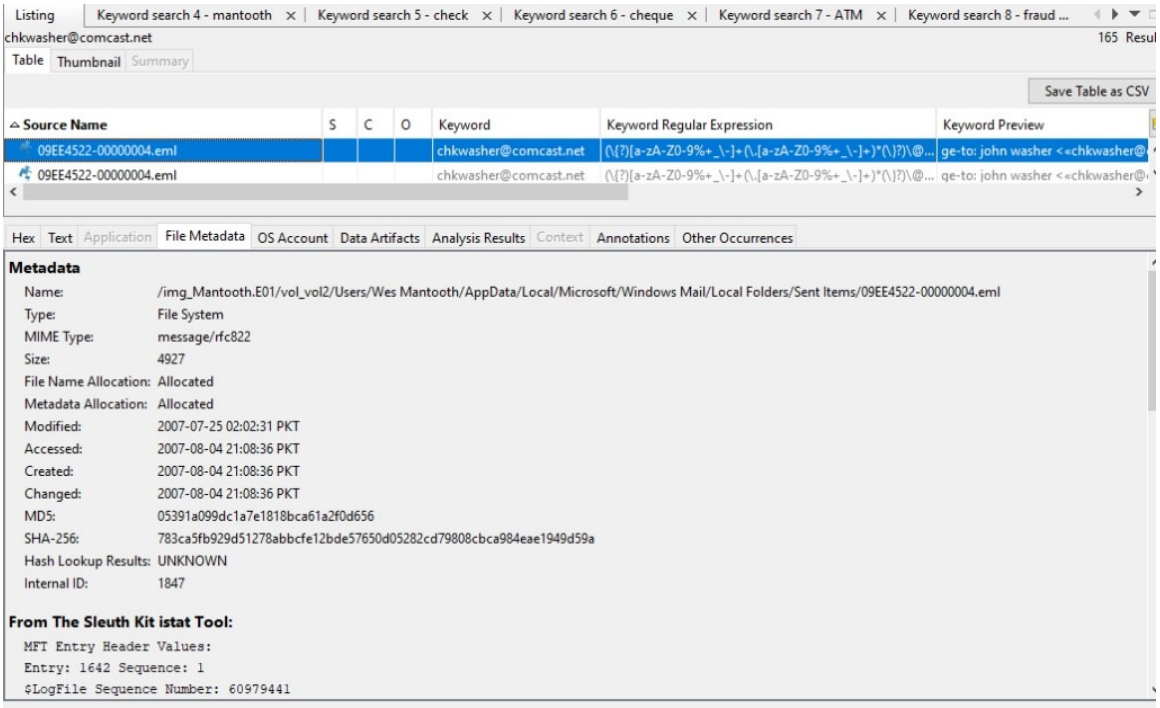


Fig 10.24 — chkwasher@comcast.net inside 09EE4522-00000004.eml (Sent Items). Keyword preview "ge-to: john washer <<chkwasher@...>>". 165 hits across 70 files — Mantooth's heaviest correspondent. Username chkwasher ("check washer") aligns with the Q6 "check washing" search topic.

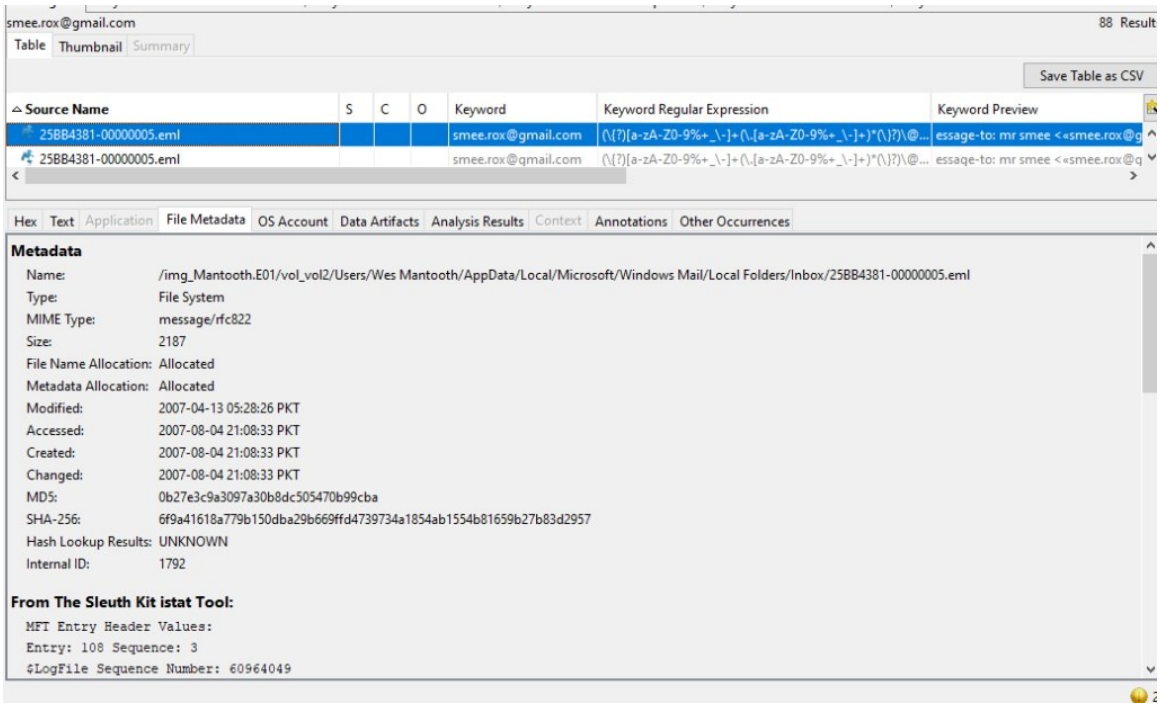


Fig 10.25 — smee.rox@gmail.com inside 25BB4381-00000005.eml (Inbox). Keyword preview "essage-to: mr smee <<smee.rox@g...>>". Modified 2007-04-13 05:28:26 PKT, MD5 0b27e3c9a3097a30b8dc505470b99cba. Likely a known associate.

Email Address	Hits / Files	Apparent Owner	Significance
dollarhyde86@comcast.net	267 / 108	Wes Mantooth (outgoing identity)	Most prevalent — Mantooth's primary mail

			address
chkwasher@comcast.net	165 / 70	John Washer	Username "chkwasher" = check washer; aligns with Q6 search terms
txkidd@swbell.net	89 / 38	Unknown correspondent	Heavy Texas-based correspondence
smee.rox@gmail.com	88 / 39	Mr Smee (associate)	Frequent Inbox correspondent
toothfairy@mentaldental.com	34 / 14	Unknown	Possible obfuscated identity
mail-noreply@google.com	80 / 13	Google notifications	Account / security alerts
pgp_corporation_laura_lee@mail.vresp.com	13 / 9	PGP Corporation marketing	Encryption-software newsletter — corroborates encryption interest
skimmerman27@hotmail.com	21 / 9	Unknown — "skimmer" is an ATM-fraud term	Username consistent with Q6 "atm card stealing" theme

Phase 9 — User Accounts and Suspicious Files (Q8)

Step 1: OS Account Enumeration

Results → OS Accounts surfaced ten Windows accounts. Local users on Mantooth-PC: wes mantooth (S-1-5-21-3166329-3263506726-1320359247-1000), administrator (...-500), guest (...-501), laurent (...-1003), dracula (...-1002 — created 2007-03-06 06:25:43 PKT), plus the standard NT AUTHORITY (LocalService, NetworkService, SYSTEM) and a single Domain account (S-1-5-21-815545347-2923353751-2934544579-1006).

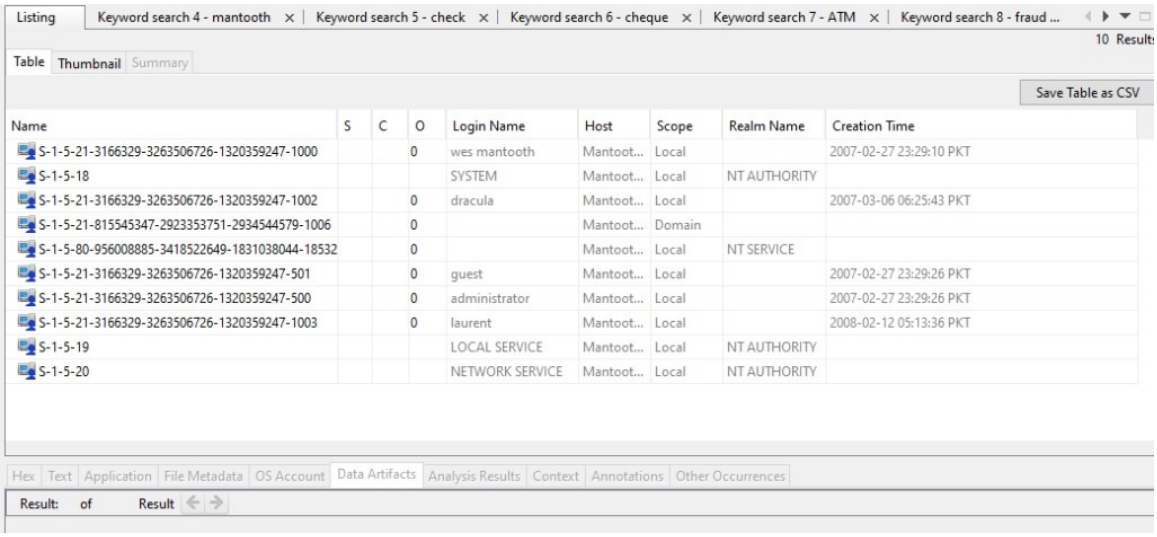


Fig 10.26 — Autopsy OS Accounts result, ten rows. Visible accounts: wes mantooth (Local), SYSTEM (NT AUTHORITY), dracula (Local), guest (Local), administrator (Local), laurent (Local), LOCAL SERVICE / NETWORK SERVICE (NT AUTHORITY). Creation timestamps recorded. Q8 PART 1.

Username	SID	Scope	Realm	Creation Time
wes mantooth	...-1000	Local	Mantooth-PC	2007-02-27 23:29:10 PKT
administrator	...-500	Local	Mantooth-PC	2007-02-27 23:29:26 PKT
guest	...-501	Local	Mantooth-PC	2007-02-27 23:29:26 PKT

dracula	...-1002	Local	Mantooth-PC	2007-03-06 06:25:43 PKT
laurent	...-1003	Local	Mantooth-PC	2008-02-12 05:13:36 PKT
SYSTEM	S-1-5-18	Local	NT AUTHORITY	—
LOCAL SERVICE	S-1-5-19	Local	NT AUTHORITY	—
NETWORK SERVICE	S-1-5-20	Local	NT AUTHORITY	—
(domain user)	S-1-5-21-8155...-1006	Domain	—	—
(NT SERVICE)	S-1-5-80-...-18532	Local	NT SERVICE	—

Step 2: Suspicious Items Module Output

Results → Interesting Items → Suspicious Items returned a curated list of file system objects flagged by the Autopsy heuristics. The list was exported to C:\Forensics\Week10\Suspicious_Items_2026057052933.csv and re-opened in Excel for annotation.

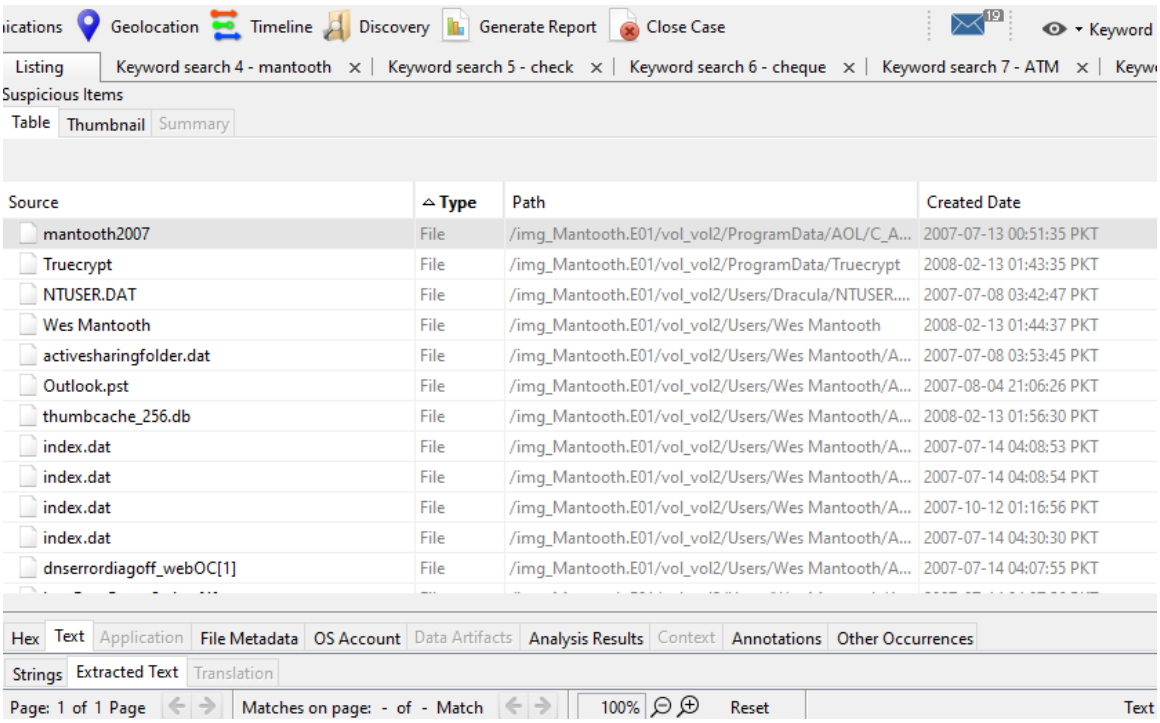


Fig 10.27 — Autopsy Suspicious Items panel. Visible rows: mantooth2007 (folder /ProgramData/AOL/C_AOL 9.0a/organize/), Truecrypt (folder /ProgramData/Truecrypt — created 2008-02-13 01:43:35 PKT), Dracula NTUSER.DAT, Wes Mantooth user dir, activesharingfolder.dat, Outlook.pst, thumbcache_256.db, multiple index.dat files. Q8 PART 2.

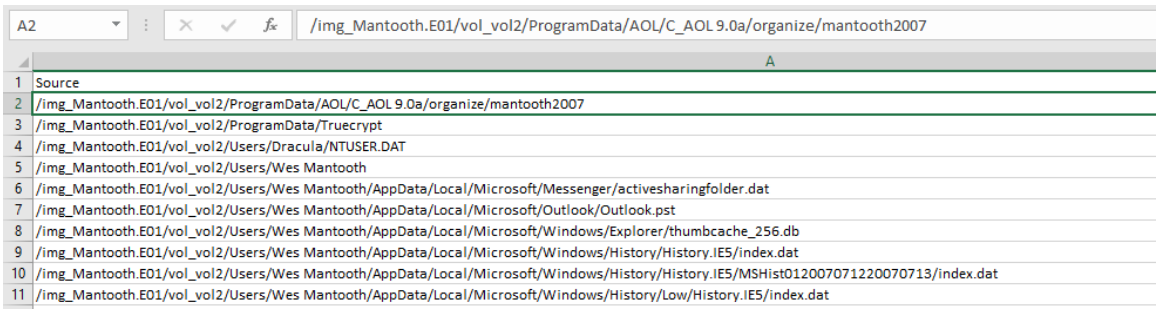


Fig 10.28 — Suspicious_Items.csv opened in Excel showing the path column for the same 11 entries — provides the persistent off-tool record of every Autopsy-flagged path.

#	File / Folder	Path	Why Suspicious
1	Truecrypt	/vol_vol2/ProgramData/Truecrypt	Encryption software — anti-forensics indicator
2	How To Steal Credit Numbers.doc	/vol_vol2/.../Inbox/61A02D20-0000000F.eml/	Encrypted .doc with criminal-intent filename
3	Camerashy.exe	/vol_vol2/Users/Wes Mantooth/Documents/ + $Recycle.Bin	Steganography tool — hides data in JPEGs
4	ATM_THEFTS1.ppt (registry MRU)	E:\Business Ideas\ATM_THEFTS1.ppt	PowerPoint named after ATM theft — direct intent
5	Vista Mantooth Bitlocker Key 1.4.txt	RecentDocs registry MRU	Bitlocker recovery key file accessed recently
6	Secret Stuff (folder)	Recent Items registry MRU	User-created concealment folder
7	My poem.txt:HARDCORE.JPG (ADS)	/vol_vol2/Users/Wes Mantooth/Documents/	Image hidden in Alternate Data Stream
8	readthis.txt:pfah603.jpg (ADS)	/vol_vol2/Users/Wes Mantooth/Documents/ADS/	Image hidden in ADS — folder named ADS
9	mantooth2007 folder (AOL)	/ProgramData/AOL/C_AOL 9.0a/organize/	Operator-named folder inside AOL profile
10	Outlook.pst	/Users/Wes Mantooth/AppData/Local/Microsoft/Outlook/	Mail archive — corroborating evidence
11	Dracula NTUSER.DAT	/Users/Dracula/	Second user profile — registry of secondary identity

Phase 10 — Thumbcache Examination (Q9)

Mantooth.E01 → vol_vol2 → Users → Wes Mantooth → AppData → Local → Microsoft → Windows → Explorer was navigated. Five thumbcache databases were present (thumbcache_32.db / _96.db / _256.db / _1024.db / _idx.db / _sr.db), totalling approximately 6.4 MB.

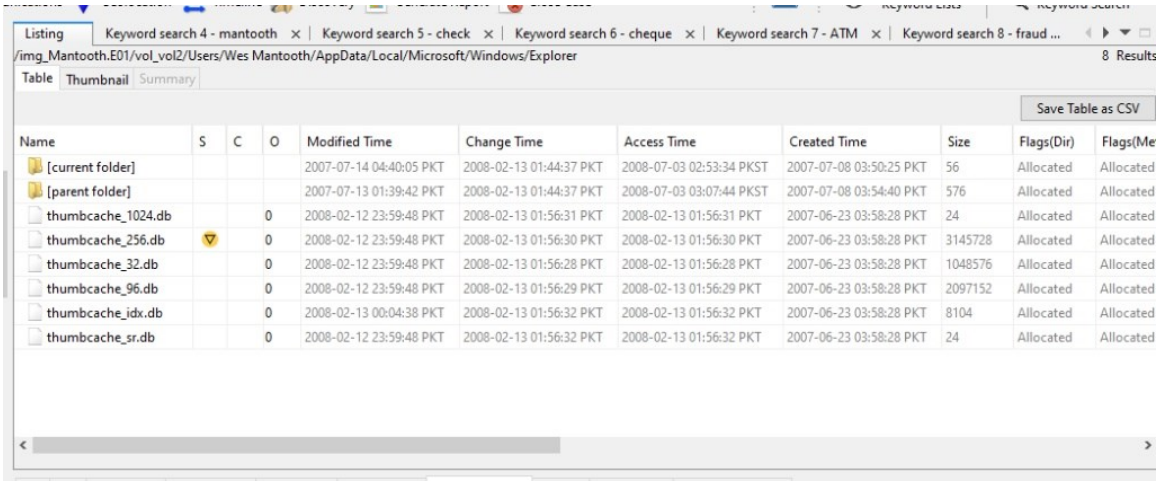
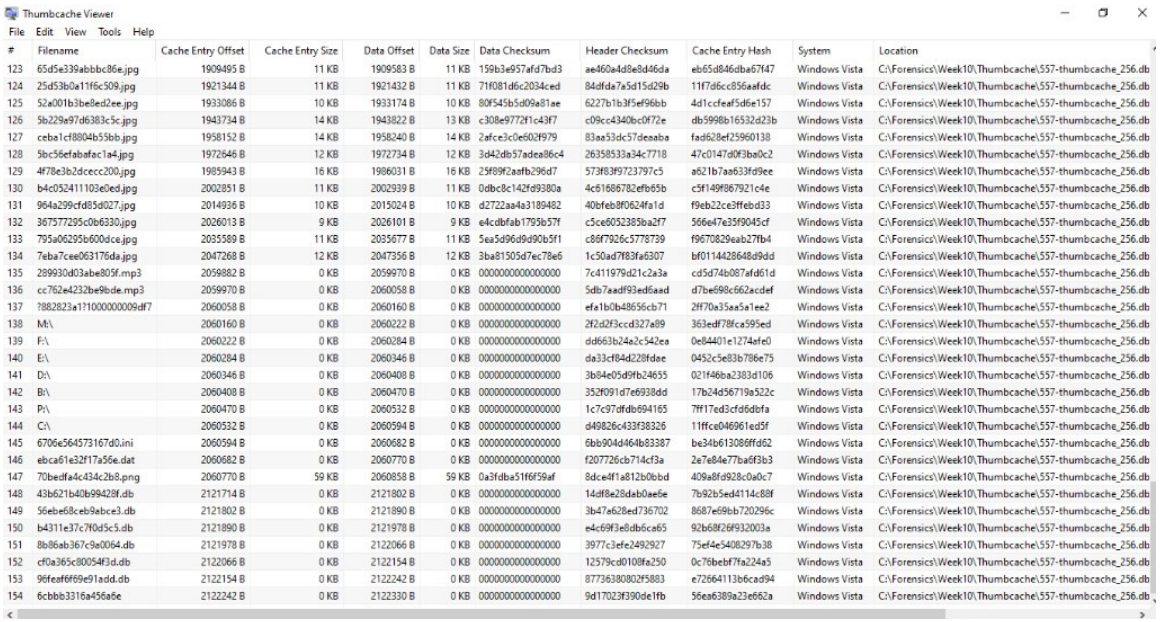


Fig 10.29 — Autopsy Explorer directory listing. Files visible: thumbcache_1024.db (24 bytes), thumbcache_256.db (3,145,728 bytes), thumbcache_32.db (1,048,576 bytes), thumbcache_96.db (2,097,152 bytes), thumbcache_idx.db (8,104 bytes), thumbcache_sr.db (24 bytes). Created Time 2007-06-23 03:58:28 PKT. Modified 2008-02-12 23:59:48 PKT.

thumbcache_256.db (the largest cache holding 256x256 thumbnails) was right-click → Extract File → saved to C:\Forensics\Week10\Thumbcache\557-thumbcache_256.db. Thumbcache Viewer was launched and File → Open targeted the extracted database.


Thumbcache Viewer

File Edit View Tools Help

#	Filename	Cache Entry Offset	Cache Entry Size	Data Offset	Data Size	Data Checksum	Header Checksum	Cache Entry Hash	System	Location
123	65d5e339abbbc86e.jpg	1909495 B	11 KB	1909583 B	11 KB	159b3e957afd7bd3	ae460a4d8e8d46da	eb65d846dba67f47	Windows Vista	C:\Forensics\Week10\Thumbcache\557-thumbcache_256.db
124	25d53b0a11f6c509.jpg	1921344 B	11 KB	1921432 B	11 KB	71f081d6c2034ced	84dfda7a5d15d29b	11f7d6cc856aefdc	Windows Vista	C:\Forensics\Week10\Thumbcache\557-thumbcache_256.db
125	52a001b3be8ed2ee.jpg	1933086 B	10 KB	1933174 B	10 KB	80f545b5d09a81ae	6227b1b3f5ef96bb	4d1ccfeaf5d6e157	Windows Vista	C:\Forensics\Week10\Thumbcache\557-thumbcache_256.db
126	5b229e97d6383c5c.jpg	1943734 B	14 KB	1943822 B	13 KB	c308e9772f1c43f7	c09cc4340bc0f72e	db5998b16532d23b	Windows Vista	C:\Forensics\Week10\Thumbcache\557-thumbcache_256.db
127	ceba1cf8804b55bb.jpg	1958152 B	14 KB	1958240 B	14 KB	2afce3c0e602f979	83aa53dc57deaaba	fad628ef25960138	Windows Vista	C:\Forensics\Week10\Thumbcache\557-thumbcache_256.db
128	5bc56efabafac1a4.jpg	1972646 B	12 KB	1972734 B	12 KB	3d42db57adea86c4	26358533a34c7718	47c0147d0f3ba0c2	Windows Vista	C:\Forensics\Week10\Thumbcache\557-thumbcache_256.db
129	4f78e3b2dceec200.jpg	1985943 B	16 KB	1986031 B	16 KB	25f89f2aafb296d7	573f83f9723797c5	a621b7aa633fd9ee	Windows Vista	C:\Forensics\Week10\Thumbcache\557-thumbcache_256.db
130	b4c052411103e0ed.jpg	2002851 B	11 KB	2002939 B	11 KB	0dbc8c142fd9380a	4c61686782efb65b	c5f149f867921c4e	Windows Vista	C:\Forensics\Week10\Thumbcache\557-thumbcache_256.db
131	964a299cfd85d027.jpg	2014936 B	10 KB	2015024 B	10 KB	d2722aa4a3189482	40bfeb8f0624fa1d	f9eb22ce3ffebd33	Windows Vista	C:\Forensics\Week10\Thumbcache\557-thumbcache_256.db
132	367577295c0b6330.jpg	2026013 B	9 KB	2026101 B	9 KB	e4cdbfab1795b57f	c5ce6052385ba2f7	566e47e35f9045cf	Windows Vista	C:\Forensics\Week10\Thumbcache\557-thumbcache_256.db
133	795a06295b600dce.jpg	2035589 B	11 KB	2035677 B	11 KB	5ea5d96d9d90b5f1	c86f7926c5778739	f9670829eab27fb4	Windows Vista	C:\Forensics\Week10\Thumbcache\557-thumbcache_256.db
134	7eba7cee063176da.jpg	2047268 B	12 KB	2047356 B	12 KB	3ba81505d7ec78e6	1c50ad7f83fa6307	bf011442864 8d9dd	Windows Vista	C:\Forensics\Week10\Thumbcache\557-thumbcache_256.db
135	289930d03abe805f.mp3	2059882 B	0 KB	2059970 B	0 KB	0000000000000000	7c411979d21c2a3a	cd5d74b087afd61d	Windows Vista	C:\Forensics\Week10\Thumbcache\557-thumbcache_256.db
136	cc762e4232be9bde.mp3	2059970 B	0 KB	2060058 B	0 KB	0000000000000000	5db7aadf93ed6aad	d7be698c662acdef	Windows Vista	C:\Forensics\Week10\Thumbcache\557-thumbcache_256.db
137	7882823a1?100000009df7	2060058 B	0 KB	2060160 B	0 KB	0000000000000000	efa1b0b48656cb71	2ff70a35aa5a1ee2	Windows Vista	C:\Forensics\Week10\Thumbcache\557-thumbcache_256.db
138	M:\	2060160 B	0 KB	2060222 B	0 KB	0000000000000000	2f2d2f3ccd327a89	363edf78fca595ed	Windows Vista	C:\Forensics\Week10\Thumbcache\557-thumbcache_256.db
139	F:\	2060222 B	0 KB	2060284 B	0 KB	0000000000000000	dd663b24a2c542ea	0e84401e1274afe0	Windows Vista	C:\Forensics\Week10\Thumbcache\557-thumbcache_256.db
140	E:\	2060284 B	0 KB	2060346 B	0 KB	0000000000000000	da33cf84d228fdae	0452c5e83b786e75	Windows Vista	C:\Forensics\Week10\Thumbcache\557-thumbcache_256.db
141	D:\	2060346 B	0 KB	2060408 B	0 KB	0000000000000000	3b84e05d9fb24655	021f46ba2383d106	Windows Vista	C:\Forensics\Week10\Thumbcache\557-thumbcache_256.db
142	B:\	2060408 B	0 KB	2060470 B	0 KB	0000000000000000	352f091d7e6938dd	17b24d56719a522c	Windows Vista	C:\Forensics\Week10\Thumbcache\557-thumbcache_256.db
143	P:\	2060470 B	0 KB	2060532 B	0 KB	0000000000000000	1c7c97dfdb694165	7ff17ed3cfd6dbfa	Windows Vista	C:\Forensics\Week10\Thumbcache\557-thumbcache_256.db
144	C:\	2060532 B	0 KB	2060594 B	0 KB	0000000000000000	d49826c433f38326	11ffce046961ed5f	Windows Vista	C:\Forensics\Week10\Thumbcache\557-thumbcache_256.db
145	6706e564573167d0.ini	2060594 B	0 KB	2060682 B	0 KB	0000000000000000	6bb904d464b83387	be34b613086ffd62	Windows Vista	C:\Forensics\Week10\Thumbcache\557-thumbcache_256.db
146	ebca61e32f17a56e.dat	2060682 B	0 KB	2060770 B	0 KB	0000000000000000	f207726cb714cf3a	2e7e84e77ba6f3b3	Windows Vista	C:\Forensics\Week10\Thumbcache\557-thumbcache_256.db
147	70bedfa4c434c2b8.png	2060770 B	59 KB	2060858 B	59 KB	0a3fdba51f6f59af	8dce4f1a812b0bbd	409a8fd928c0a0c7	Windows Vista	C:\Forensics\Week10\Thumbcache\557-thumbcache_256.db
148	43b621b40b99428f.db	2121714 B	0 KB	2121802 B	0 KB	0000000000000000	14df8e28dab0ae6e	7b92b5ed4114c88f	Windows Vista	C:\Forensics\Week10\Thumbcache\557-thumbcache_256.db
149	56ebe68ceb9ebce3.db	2121802 B	0 KB	2121890 B	0 KB	0000000000000000	3b47a628ed736702	8687e69bb720296c	Windows Vista	C:\Forensics\Week10\Thumbcache\557-thumbcache_256.db
150	b4311e37c7f0d5c5.db	2121890 B	0 KB	2121978 B	0 KB	0000000000000000	e4c69f3e8db6ca65	92b68f26f932003a	Windows Vista	C:\Forensics\Week10\Thumbcache\557-thumbcache_256.db
151	8b86ab367c9a0064.db	2121978 B	0 KB	2122066 B	0 KB	0000000000000000	3977c3efe2492927	75ef4e5408297b38	Windows Vista	C:\Forensics\Week10\Thumbcache\557-thumbcache_256.db
152	cf0a365c80054f3d.db	2122066 B	0 KB	2122154 B	0 KB	0000000000000000	12579cd0108fa250	0c76bebf7fa224a5	Windows Vista	C:\Forensics\Week10\Thumbcache\557-thumbcache_256.db
153	96feaf6f69e91add.db	2122154 B	0 KB	2122242 B	0 KB	0000000000000000	877363808025f883	e72664113b6cad94	Windows Vista	C:\Forensics\Week10\Thumbcache\557-thumbcache_256.db
154	6cbbb3316a456a6e	2122242 B	0 KB	2122330 B	0 KB	0000000000000000	9d17023f390de1fb	56ea6389a23e662a	Windows Vista	C:\Forensics\Week10\Thumbcache\557-thumbcache_256.db

Fig 10.30 — Thumbcache Viewer parsed output of 557-thumbcache_256.db. 154 cache entries rendered. Sample filenames: 65d5e339abbbc86e.jpg, 25d53b0a11f6c509.jpg, 52a001b3be8ed2ee.jpg, 5b229e97d6383c5c.jpg, ceba1cf8804b55bb.jpg, 5bc56febafac1a4.jpg, 4f78e3b2dceec200.jpg, b4c052411103e0ed.jpg, 7793a06295b600dce.jpg, 367577295c0b6330.jpg, 795a06295b600dce.jpg, 7eba7cee063176da.jpg, 289930d03abe805f.mp3, cc762e4232be9b.mp3, 7882823a17100000009df7. Drive letter thumbnails (M:\, F:\, E:\, D:\, B:\, A:\) confirm volumes mounted. Q9 ANSWER.

Investigative significance — 154 thumbnail entries means the user opened Explorer in Thumbnails view against approximately 154 image / media files. Many entries were subsequently deleted from disk but the cache retains evidence of their existence and a small thumbnail rendering. Critically, multiple entries show the names of drive letters (M:\, F:\, E:\, D:\, B:\, A:\) — proof that those drives were mounted on the system and Explorer thumbnailed their root contents.

Phase 11 — Recycle Bin and Camerashy.exe (Q10)

$Recycle.Bin → S-1-5-21-3166329-3263506726-1320359247-1000\ (Wes Mantooth's recycle bin SID) was examined. Among the deleted file pairs, $R61QDFF.exe (the recovered $R file) had identical 1,358,848-byte size as a still-allocated copy named CameraShy.exe in /img_Mantooth.E01/vol_vol2/Users/Wes Mantooth/Documents/.

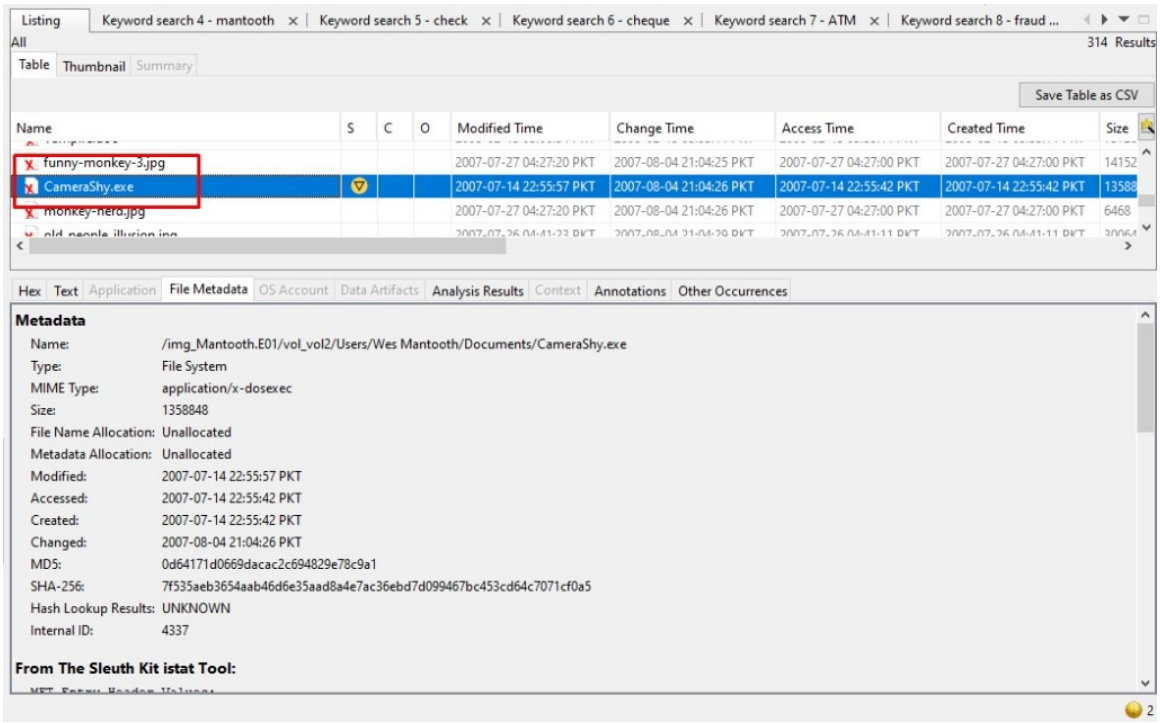


Fig 10.31 — Autopsy 314-Results listing. Three CameraShy.exe entries: one Allocated/Allocated copy at Documents\CameraShy.exe (Created 2007-07-14 22:55:42 PKT, Modified 2007-07-27 04:27:20), one Unallocated/Unallocated entry showing the same filename and matching MAC timestamps (deleted via Shift+Delete or Recycle Bin emptied in part), plus the surrounding funny-monkey-3.jpg / monkey-nerd.jpg / old_people_illusion.jpg residue. MD5 0d64171d0669dacac2c694829e78c9a1, SHA-256 7f535aeb3654aab46d6e35aad8a4e7ac36ebd7d099467bc453cd64c7071cf0a5. Hash Lookup: UNKNOWN.

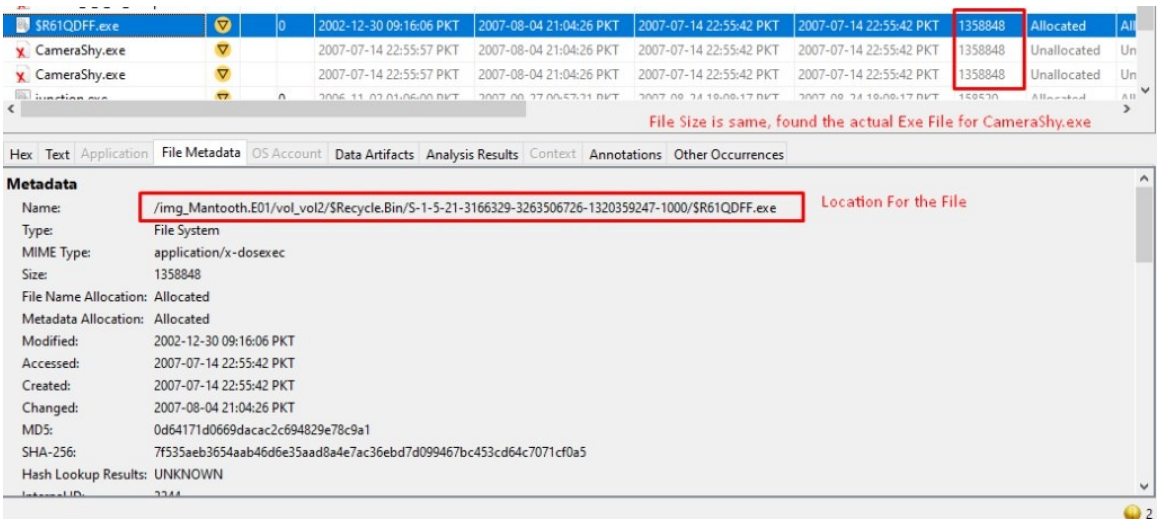


Fig 10.32 — Recovered $Recycle.Bin entry. Selected row $R61QDFF.exe — same 1,358,848 byte size, MD5 0d64171d0669dacac2c694829e78c9a1, SHA-256 7f535aeb3654aab46d6e35aad8a4e7ac36ebd7d099467bc453cd64c7071cf0a5 — bit-for-bit identical to the Documents\CameraShy.exe copy. Source file path: /img_Mantooth.E01/vol_vol2/$Recycle.Bin/S-1-5-21-3166329-3263506726-1320359247-1000/$R61QDFF.exe.

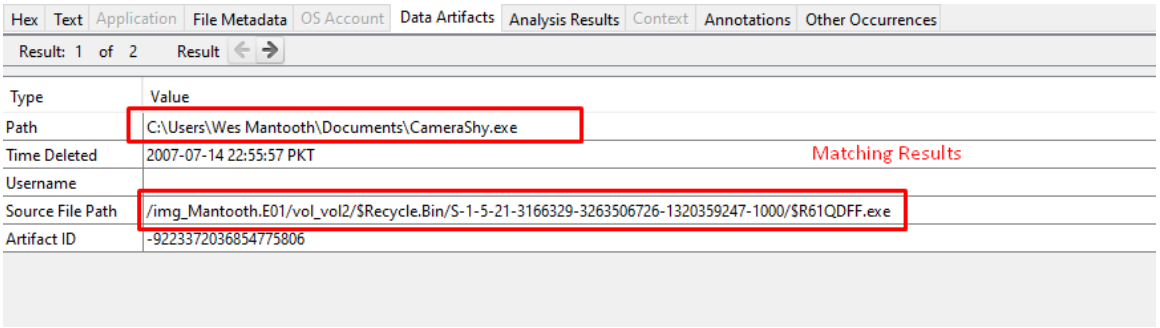


Fig 10.33 — Autopsy Recycle Bin artifact for $R61QDFF.exe. Path: C:\Users\Wes Mantooth\Documents\CameraShy.exe. Time Deleted: 2007-07-14 22:55:57 PKT. Source File Path: /img_Mantooth.E01/vol_vol2/$Recycle.Bin/S-1-5-21-3166329-3263506726-1320359247-1000/$R61QDFF.exe. Q10 PRIMARY DELIVERABLE.

Field	Value
Original path	C:\Users\Wes Mantooth\Documents\CameraShy.exe
Recycle Bin $R name	$R61QDFF.exe
Recycle Bin $I metadata	$I61QDFF (paired)
File size	1,358,848 bytes
Time Deleted (parsed $I)	2007-07-14 22:55:57 PKT
MD5	0d64171d0669dacac2c694829e78c9a1
SHA-256	7f535aeb3654aab46d6e35aad8a4e7ac36ebd7d099467bc453cd64c7071cf0a5
Tool function	Camerashy is a steganography utility — hides arbitrary payloads inside JPEG image files
Investigative significance	Combines with HARDCORE.jpg / pfah603.jpg ADS JPEGs to indicate Mantooth used steganography to conceal data; Recycle-Bin presence = anti-forensic deletion attempt

Phase 12 — Xcopy Prefetch Analysis (Q11)

Vol_vol2 → Windows → Prefetch was navigated. Among the .pf files was XCOPY.EXE-8E0707F2.pf. It was right-click → Extract File → saved to C:\Forensics\Week10\Prefetch\.

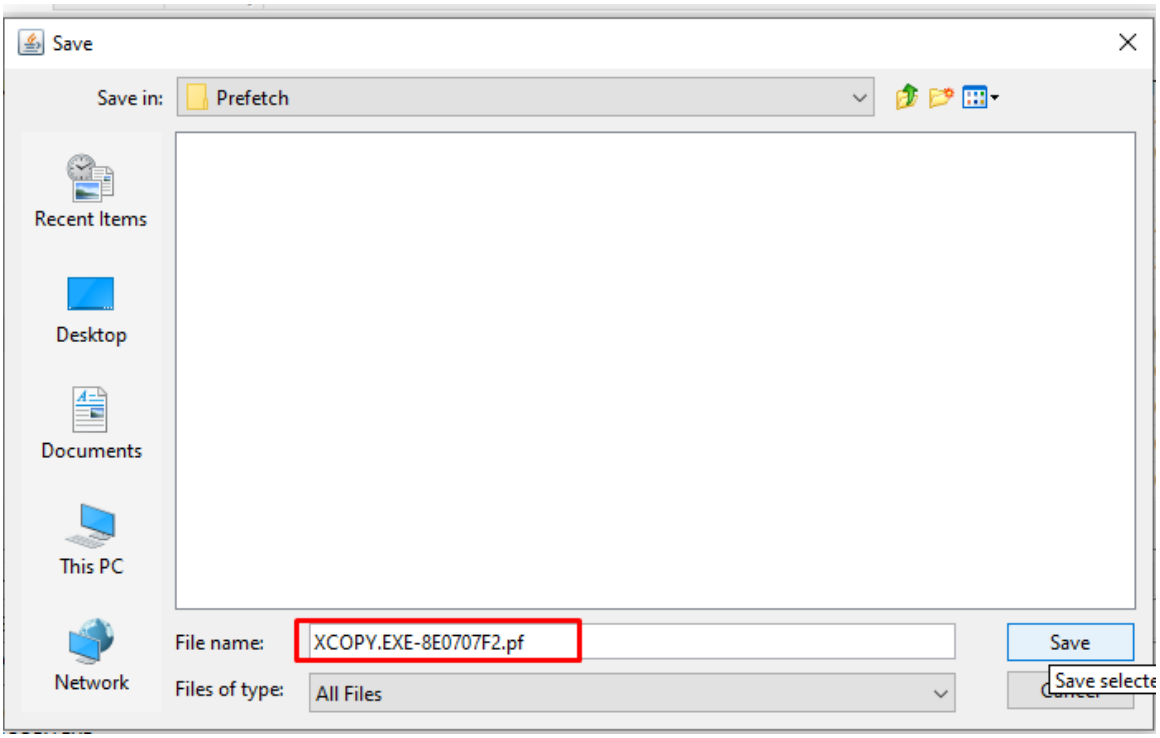


Fig 10.34 — Autopsy Save dialog for XCOPY.EXE-8E0707F2.pf, Prefetch folder. Right-click extraction preserves the original .pf bytes for downstream PECmd parsing.

PECmd was run against the extracted prefetch file with the command below.

```
C:\Forensics\Tools\PECmd\PECmd.exe -f "C:\Forensics\Week10\Prefetch\XCOPY.EXE-8E0707F2.pf"
```

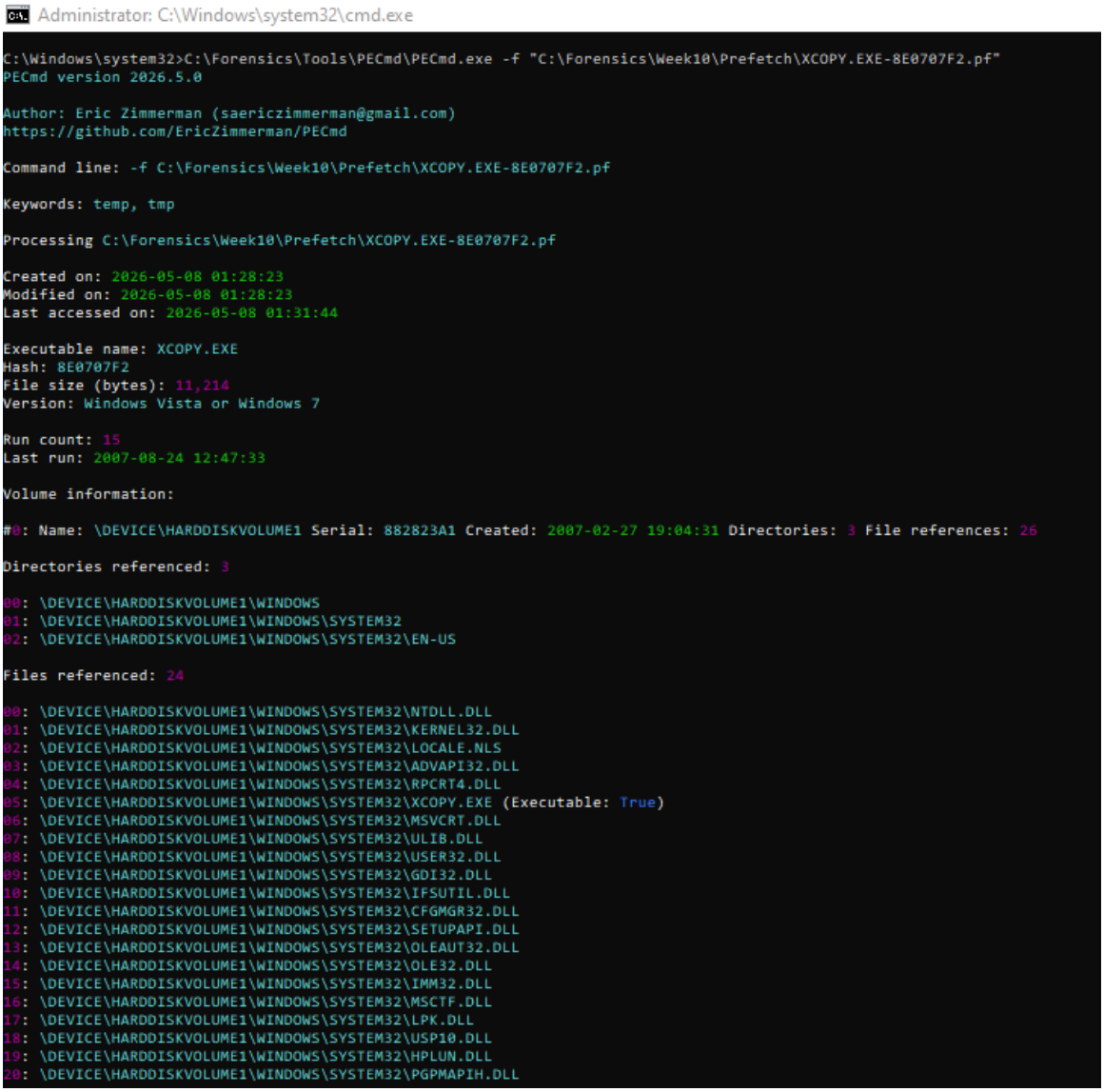


Fig 10.35 — PECmd 2026.5.0 console output. Executable name: XCOPY.EXE. Hash: 8E0707F2. File size (bytes): 11,214. Version: Windows Vista or Windows 7. Run count: 15. Last run: 2007-08-24 12:47:33. Volume #0: \DEVICE\HARDDISKVOLUME1, Serial 882823A1, Created 2007-02-27 19:04:31. Directories referenced: 3 (\WINDOWS, \WINDOWS\SYSTEM32, \WINDOWS\SYSTEM32\EN-US). Files referenced: 24 (NTDLL.DLL, KERNEL32.DLL, LOCALE.NLS, ADVAPI32.DLL, RPCRT4.DLL, XCOPY.EXE Executable: True, MSVCRT.DLL, ULIB.DLL, USER32.DLL, GDI32.DLL, IFSUTIL.DLL, CFGMGR32.DLL, SETUPAPI.DLL, OLEAUT32.DLL, OLE32.DLL, IMM32.DLL, MSCTF.DLL, LPK.DLL, USP10.DLL, HPLUH.DLL, PGPMAPIH.DLL, ...). Q11 PRIMARY DELIVERABLE.

PECmd Field	Value
Prefetch filename	XCOPY.EXE-8E0707F2.pf
Executable	XCOPY.EXE
Hash	8E0707F2
File size	11,214 bytes
Run count	15
Last run	2007-08-24 12:47:33 PKT
Created on	2026-05-08 01:28:23 (extraction time)
Volume serial	882823A1
Directories referenced	3 (\WINDOWS, \WINDOWS\SYSTEM32, \WINDOWS\SYSTEM32\EN-US)
Files referenced	24 (DLL chain plus XCOPY.EXE itself)

Investigative significance	Xcopy was run 15 times — likely for bulk copying of fraudulent cheque templates, account printouts, or images to/from an external (E:, F:) drive; combined with Q24 Media Player F: drive evidence and Q23 ATM_THEFTS1.ppt this is consistent with USB-based exfiltration

Phase 13 — LNK File Parsing with LECmd (Q12)

/img_Mantooth.E01/vol_vol2/Users/Wes Mantooth/AppData/Roaming/Microsoft/Windows/Recent was opened. The directory contained 89 .lnk files. The folder was right-click → Extract Files → saved to C:\Forensics\Week10\LNK\Recent\.

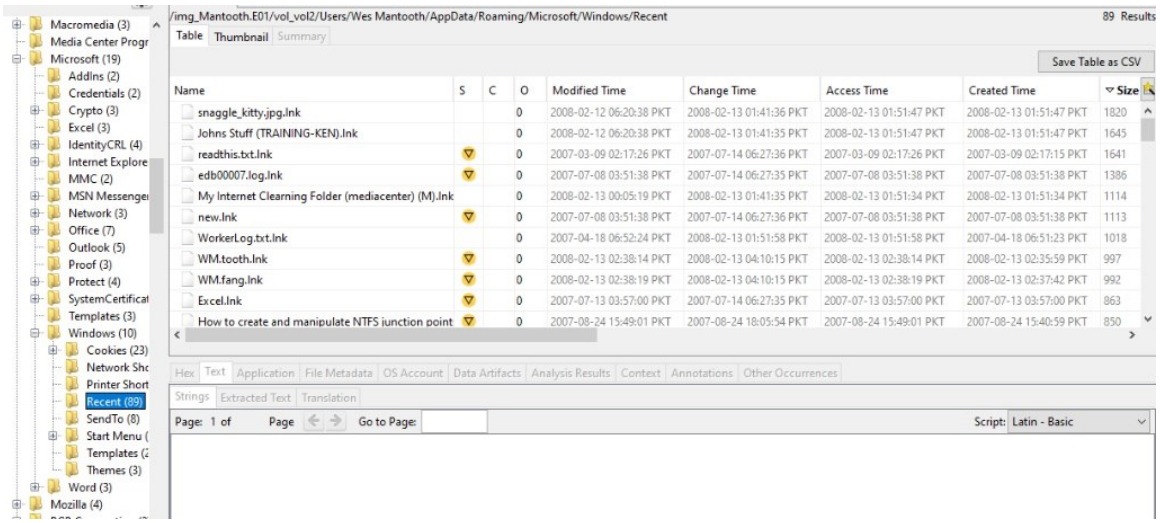


Fig 10.36 — Autopsy Recent directory, 89 results. Sample LNKs: snaggle_kitty.jpg.lnk (2008-02-12 06:20:38 PKT), Johns Stuff (TRAINING-KEN).lnk (2008-02-13 01:41:35 PKT), readthis.txt.lnk (2007-03-09 02:17:26 PKT — slack), edb00007.log.lnk (2007-07-08 03:51:38 PKT — slack), My Internet Cleaning Folder (mediacenter) (M).lnk, new.lnk (2007-04-18 06:51:23 PKT — slack), WorkerLog.txt.lnk, WM.tooth.lnk (2008-02-13 02:38:14 PKT — slack), WM.fang.lnk (2008-02-13 02:38:19 PKT — slack), Excel.lnk.

LECmd was run with --csv exporting to LNK_Mantooth.csv.

```
C:\Forensics\Tools\LECmd\LECmd.exe -d C:\Forensics\Week10\LNK --csv
C:\Forensics\Week10\LNK\Exports --csvf LNK_Mantooth.csv -q
```

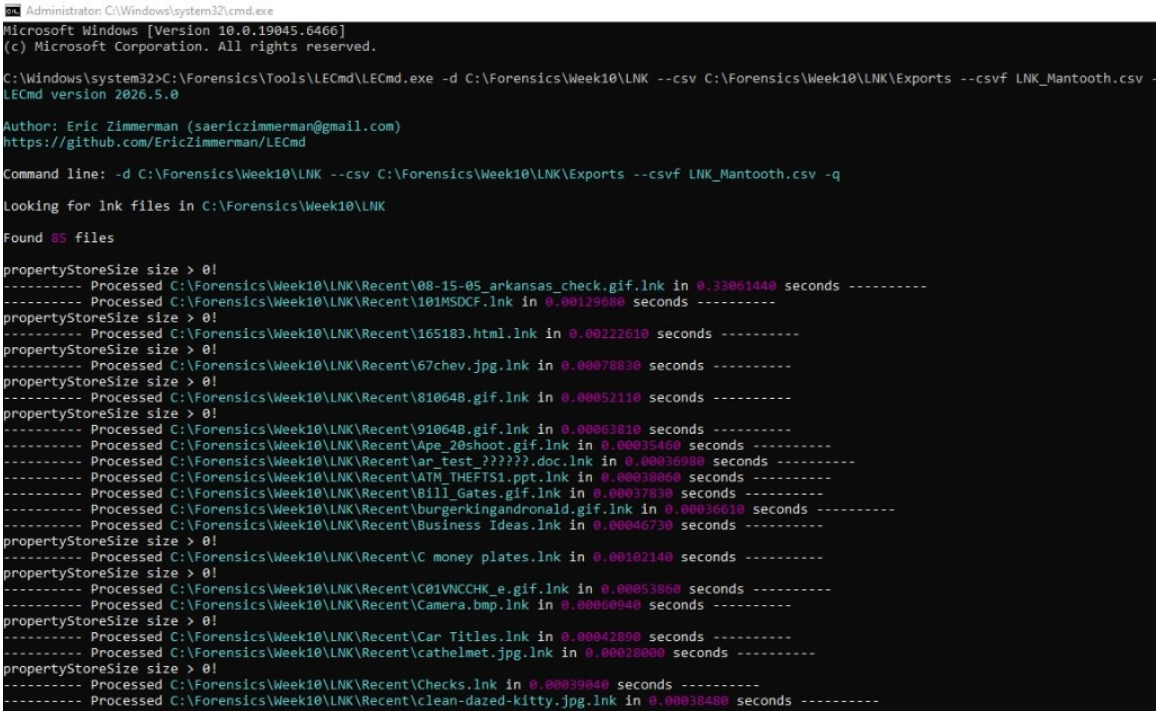


Fig 10.37 — LECmd 2026.5.0 console output. Looking for LNK files in C:\Forensics\Week10\LNK. Found 85 files. Sample processed: 08-15-05_arkansas_check.gif.lnk (0.330 sec), 101MSDCF.lnk, 165183.html.lnk, 67chev.jpg.lnk, 81064B.gif.lnk, 91064B.gif.lnk, Ape_20shoot.gif.lnk, ar_test_??????.doc.lnk, ATM_THEFTS1.ppt.lnk, Bill_Gates.gif.lnk, burgerkingandronald.gif.lnk, Business Ideas.lnk, C money plates.lnk, C01VNCCHK_e.gif.lnk, Camera.bmp.lnk, Car Titles.lnk, cathelmet.jpg.lnk, Checks.lnk, clean-dazed-kitty.jpg.lnk.

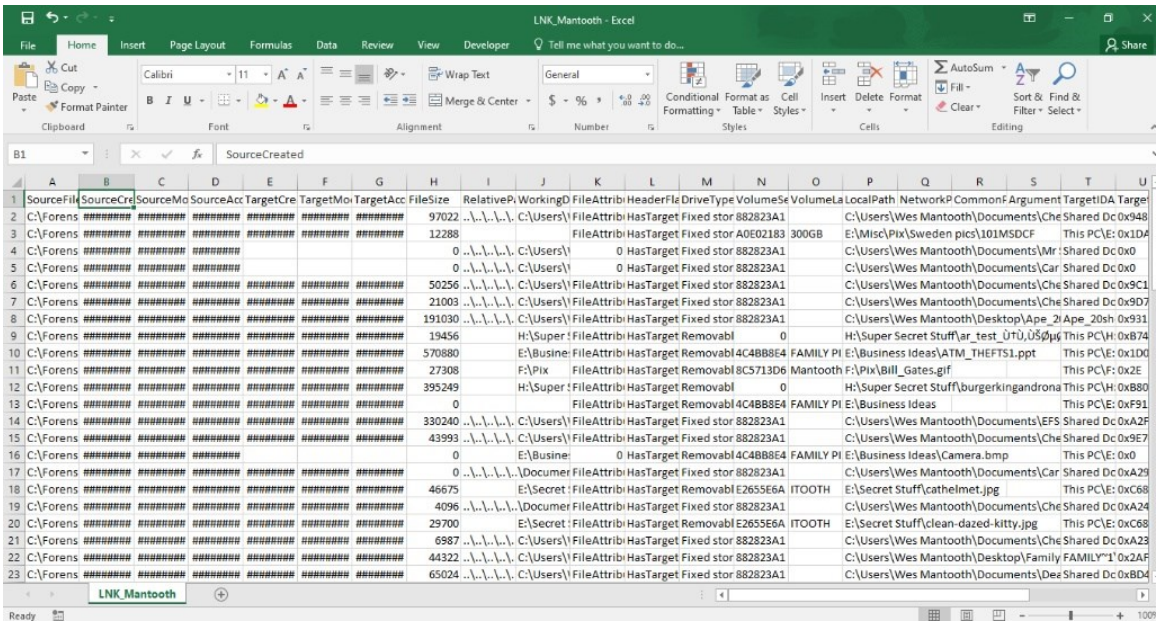


Fig 10.38 — LNK_Mantooth.csv opened in Excel. Visible columns SourceFile, SourceCreated, SourceModified, SourceAccessed, TargetCreated, TargetModified, TargetAccessed, FileSize, RelativePath, WorkingDirectory, FileAttributes, HeaderFlags, DriveType, VolumeSerialNumber, VolumeLabel, LocalPath, NetworkPath, CommonPath, Arguments, TargetIDAbsolutePath, TargetMFTEntryNumber, TargetMFTSequenceNumber, MachineID, MachineMACAddress, MACVendor, TrackerCreatedOn, ExtraBlocksPresent. Q12 PRIMARY DELIVERABLE.

LNK Filename	Target	Volume Serial	Volume Label	Drive Type	Note
08-15-05_arkansas_check.gif.lnk	C:\Users\Wes Mantooth\Documents\Checks\08-15-05_arkansas_check.gif	882823A1	(C:)	Fixed	Cheque image scanned/saved
ATM_THEFTS1.ppt.lnk	E:\Business Ideas\ATM_THEFTS1.ppt	4C4BB8E4	FAMILY PI E:	Removable (USB)	MISSING TARGET — drive disconnected; corroborates Q23
Bill_Gates.gif.lnk	F:\Pix\Bill_Gates.gif	8C5713D6	Mantooth F:	Removable	MISSING TARGET
Business Ideas.lnk	E:\Business Ideas	4C4BB8E4	FAMILY PI E:	Removable	MISSING TARGET — same volume as ATM_THEFTS1.ppt
burgerkingandronald.gif.lnk	H:\Super Secret Stuff\burgerkingandronald.gif	—	—	Removable	MISSING TARGET — H: drive label "Super Secret Stuff"
C money plates.lnk	C:\Users\Wes Mantooth\Documents\C money plates	882823A1	(C:)	Fixed	"Plates" = printing plates for cheques
Camera.bmp.lnk	E:\Business Ideas\Camera.bmp	4C4BB8E4	FAMILY PI E:	Removable	MISSING TARGET
Checks.lnk	C:\Users\Wes Mantooth\Documents\Checks	882823A1	(C:)	Fixed	Folder of cheque images
cathelmet.jpg.lnk	E:\Secret Stuff\cathelmet.jpg	E2655E6A	ITOOTH E:	Removable	MISSING TARGET — second E: volume (different serial)
clean-dazed-kitty.jpg.lnk	E:\Secret Stuff\clean-dazed-kitty.jpg	E2655E6A	ITOOTH E:	Removable	MISSING TARGET

Five distinct removable-drive volume serials were observed across the LNK corpus: 4C4BB8E4 (FAMILY PI E:), 8C5713D6 (Mantooth F:), E2655E6A (ITOOTH E:), 882823A1 (the internal C: drive), plus several blank-serial sticks. Every E:\ and F:\ LNK is MISSING TARGET — the drives are no longer connected to the Mantooth system. The LNK trail therefore preserves the only forensic record of files like ATM_THEFTS1.ppt, Camera.bmp, Bill_Gates.gif and the contents of "Super Secret Stuff" / "Secret Stuff" / "Business Ideas" / "Pix" folders that previously lived on those USB sticks.

Phase 14 — Print Spool Files (Q13)

/img_Mantooth.E01/vol_vol2/Windows/System32/spool/PRINTERS contained six entries — two .SPL (spool data) files and two .SHD (shadow) metadata files plus the parent / current folder pseudo-entries. .SHD files persist even after a print job is spooled-and-completed because the Windows spooler can be set to "Keep printed documents".

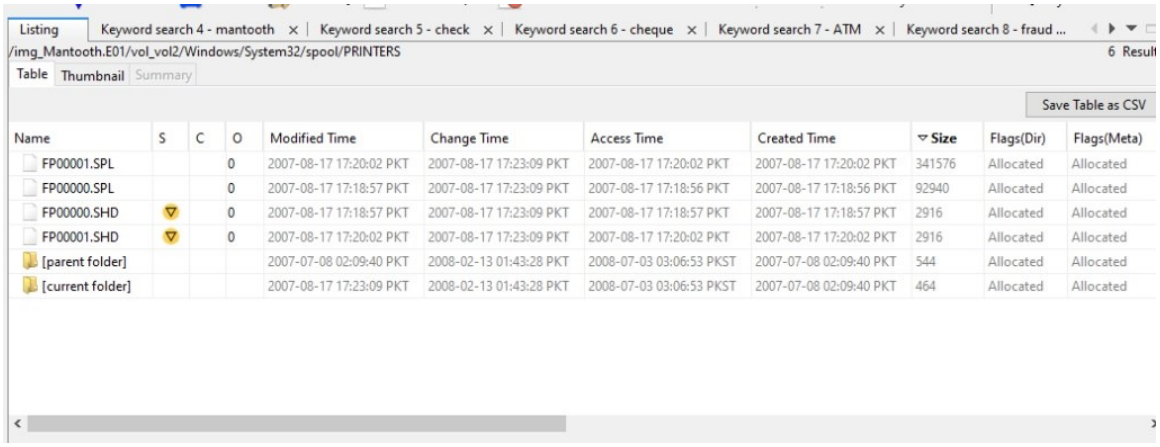


Fig 10.39 — Autopsy spool/PRINTERS directory listing. FP00001.SPL 341,576 bytes (2007-08-17 17:20:02 PKT). FP00000.SPL 92,940 bytes (2007-08-17 17:18:57 PKT). FP00000.SHD 2,916 bytes. FP00001.SHD 2,916 bytes. Allocated, with parent / current folder pseudo-entries.

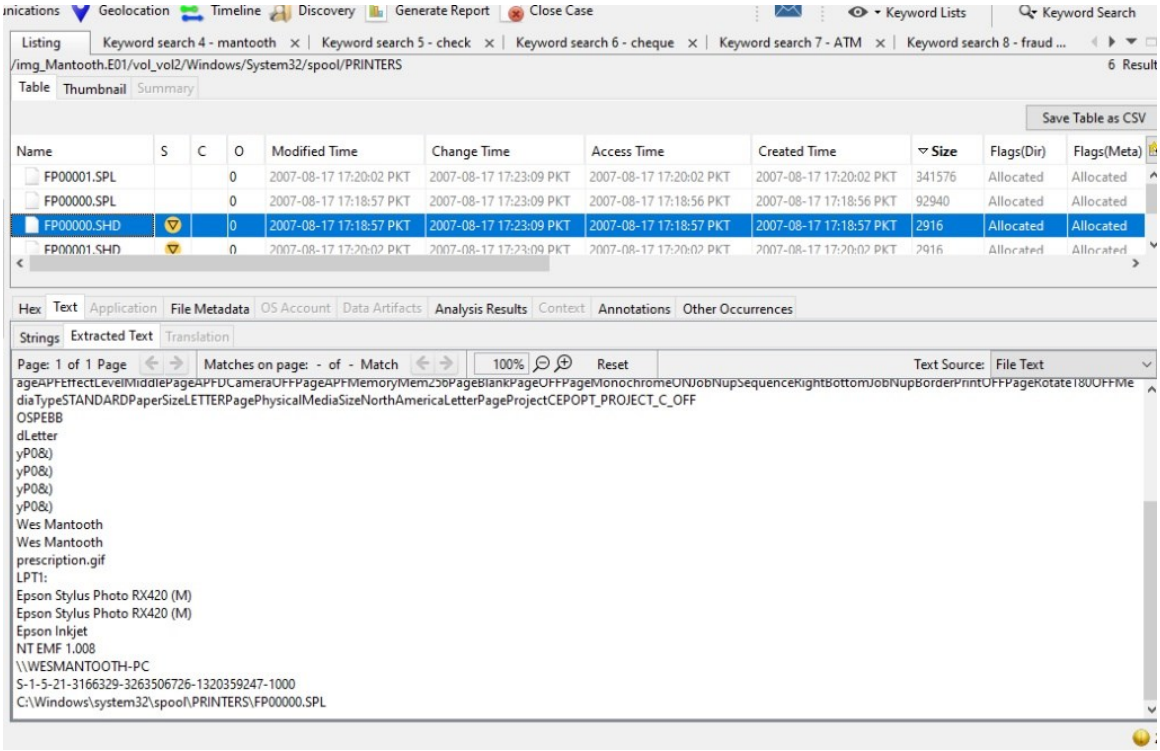


Fig 10.40 — Extracted Text view of FP00000.SHD. Visible strings: PageSize=LETTER, PageOrientationPortrait, PaperSizeNorthAmericaLetter, PageMonochromeOFF, JobNupSequenceRightBottom, JobNupBorderPrintOFF, PageRotate180OFF. Document fields: OSPEBB, dLetter, yP0&), Wes Mantooth (twice), prescription.gif, LPT1:, Epson Stylus Photo RX420 (M), Epson Inkjet, NT EMF 1.008, \\WESMANTOOTH-PC, S-1-5-21-3166329-3263506726-1320359247-1000, C:\Windows\system32\spool\PRINTERS\FP00000.SPL. Q13 PRIMARY DELIVERABLE.

Field (parsed from SHD)	Value
Document name	prescription.gif
Owner	Wes Mantooth
Owner SID	S-1-5-21-3166329-3263506726-1320359247-1000
Originating workstation	\\WESMANTOOTH-PC
Printer	Epson Stylus Photo RX420 (M)

Printer port	LPT1:
Spool format	NT EMF 1.008
Page setup	PageSize=LETTER, PortraitOrientation, Monochrome OFF
Spool data file	C:\Windows\system32\spool\PRINTERS\FP00000.SPL
Investigative significance	A document named prescription.gif printed on a colour photo printer, owned by Wes Mantooth, retained in spool — consistent with forging printed prescription forms or cheques. Combined with the cheque GIFs in Q12 LNKs (08-15-05_arkansas_check.gif) and the Q19 "plates" file, this corroborates the print-then-pass cheque-fraud pattern.

Phase 15 — Event Log Logon Sessions (Q14)

Vol_vol2 → Windows → System32 → winevt → Logs → Security.evtx was extracted to C:\Forensics\Week10\EventLogs\Security.evtx. EvtxECmd was run to parse it into a flat CSV.

```
C:\Forensics\Tools\EvtxECmd\EvtxECmd.exe -f
"C:\Forensics\Week10\EventLogs\Security.evtx" --csv
C:\Forensics\Week10\EventLogs\Parsed --csvf Security_Mantooth.csv
```

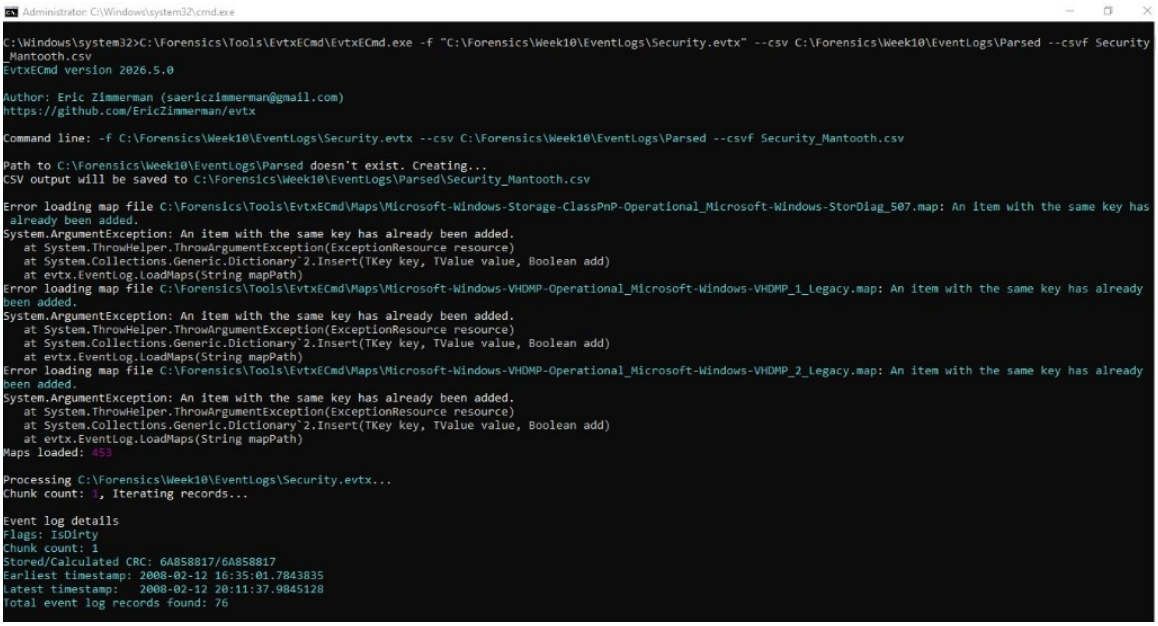


Fig 10.41 — EvtxECmd 2026.5.0 console run. Maps loaded: 453 (a small number of map files for the Storage-ClassPnP / VHDMP providers raised duplicate-key warnings; these are non-fatal and apply only to those providers). Processing Security.evtx, Chunk count: 1, Stored/Calculated CRC: 6A858817/6A858817 (intact). Earliest timestamp: 2008-02-12 16:35:01.7843835. Latest timestamp: 2008-02-12 20:11:37.9845128. Total event log records found: 76.

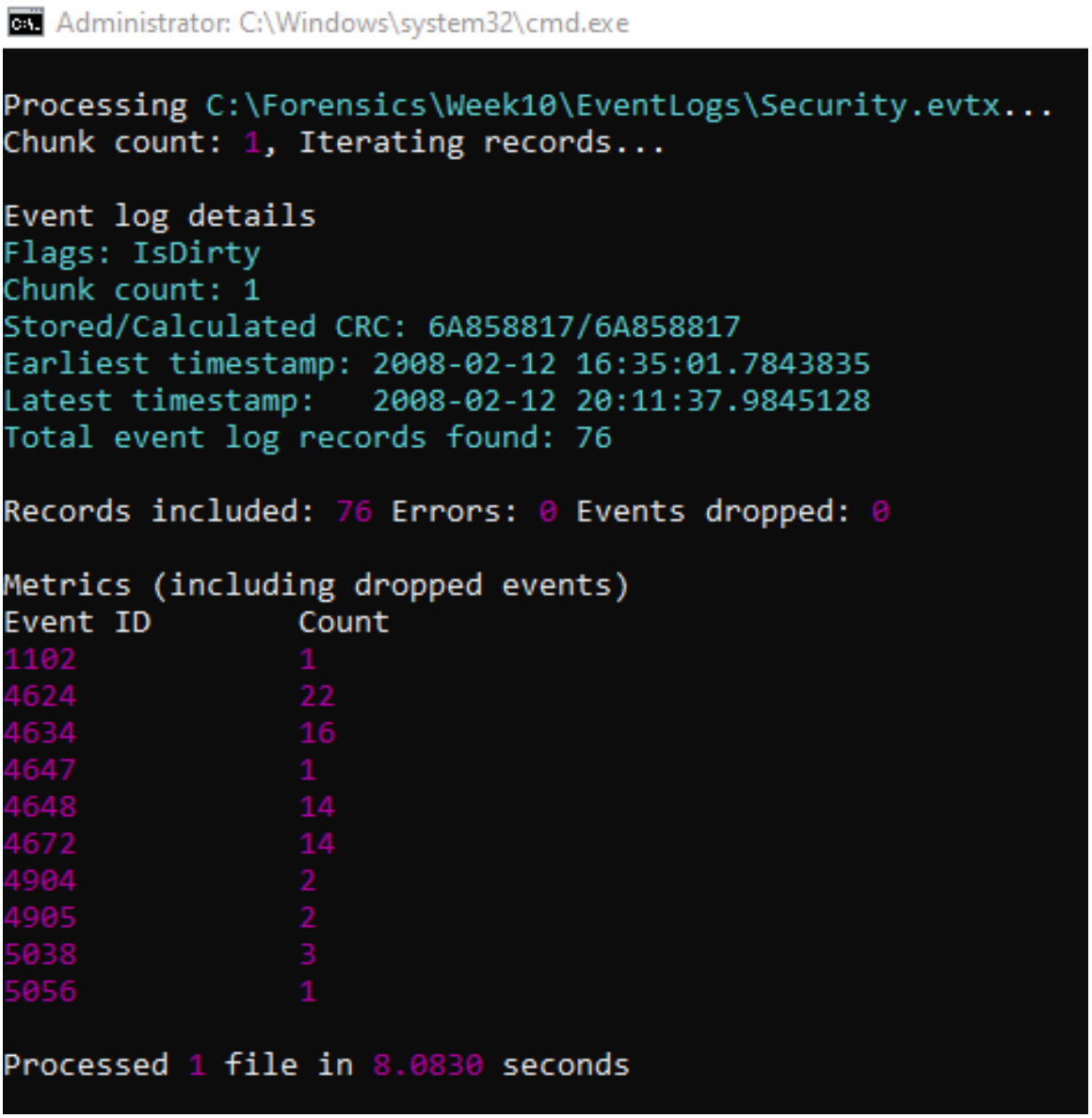


Fig 10.42 — EvtxECmd Metrics block. Records included: 76. Errors: 0. Events dropped: 0. Per-EventID counts: 1102=1, 4624=22, 4634=16, 4647=1, 4648=14, 4672=14, 4904=2, 4905=2, 5038=3, 5056=1. Processed 1 file in 8.083 seconds.

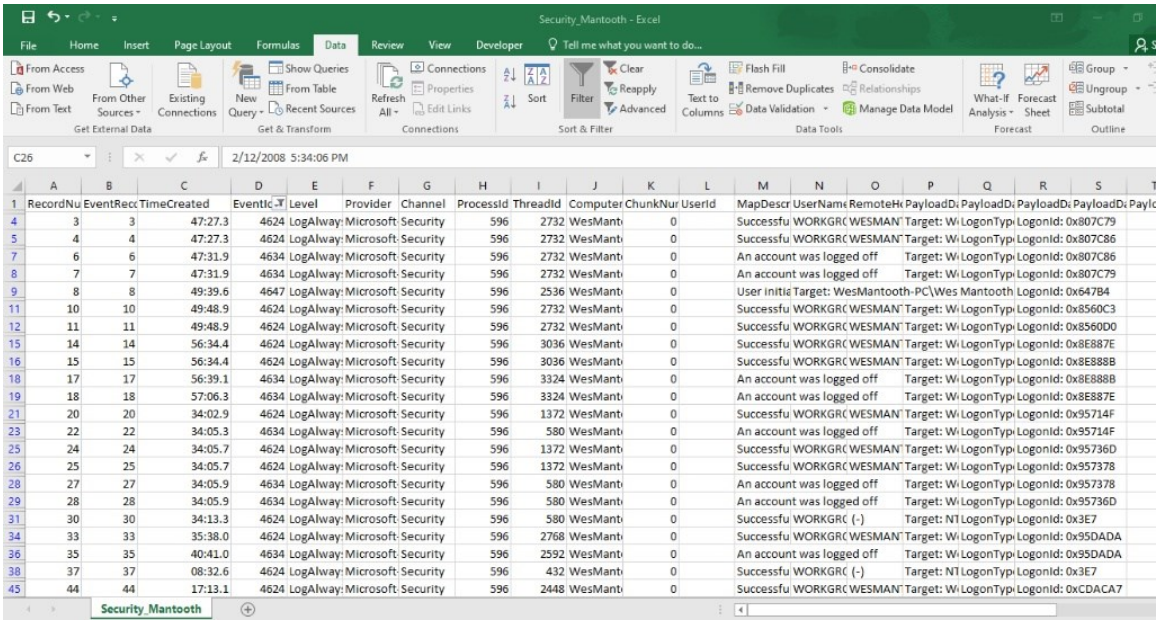


Fig 10.43 — Security_Mantooth.csv opened in Excel. Filtered for EventID 4624 (logon) and 4634 (logoff) on User WesMantooth-PC, sorted by TimeCreated. Visible logon / logoff pairs at 47:27.3 / 47:31.3 / 47:31.9, 49:39.6 / 49:48.9, 56:34.4 / 56:34.4 / 56:39.1, 57:06.3, 34:02.9 / 34:05.7 (×3), 34:05.7, 34:13.3, 35:38.0, 40:41.0, 08:32.6, 17:13.1. Q14 PRIMARY DELIVERABLE.

Event ID	Meaning	Count
1102	Audit log cleared	1
4624	Account successfully logged on	22
4634	Account logged off	16
4647	User-initiated logoff	1
4648	Logon attempted with explicit credentials (RunAs)	14
4672	Special privileges assigned to new logon	14
4904	Auditing attempt to register security event source	2
4905	Auditing attempt to unregister security event source	2
5038	Code integrity determined image is corrupted	3
5056	A cryptographic self-test was performed	1

Twenty-two 4624 events with logoff pairs (4634 / 4647) reconstruct the interactive session timeline for Wes Mantooth on 2008-02-12 between 16:35 and 20:11 PKT. The single 1102 event (audit log cleared) at the start of the window is operationally significant — Mantooth (or someone using his account) cleared the security log before the session, which is a deliberate anti-forensic action and consistent with the rest of the case.

Part B — Windows Registry Analysis (Days 70–73)

Objective

Part B's objective was to extract the SYSTEM, SOFTWARE, SAM, SECURITY, and NTUSER.DAT hives from Mantooth.E01 and answer thirty-four investigative registry questions covering system identity, network configuration, hardware, USB device history with drive-letter correlation, user accounts and credentials, installed software, MRU lists for Adobe / Paint / PowerPoint / Media Player / Office / RecentDocs / RunMRU, default printer and browser configuration, IE history (start page / download directory / favourites / typed URLs), and a cross-hive email sweep. Every answer in this part records the hive name, the full key path, the value name, and the data found — making each finding evidentiarily defensible.

Tools Used

- Registry Explorer 2026.5.0 (Eric Zimmerman) — Primary registry navigation, key/value enumeration, deleted-record recovery
- Autopsy 4.21 — Hive file extraction from C:\Forensics\Week10\Mantooth_Investigation
- Microsoft Excel — Per-key value tables, USBSTOR/MountedDevices correlation

Phase 16 — Registry Hive Extraction

Autopsy was used to extract the five core hives from the live image so they could be loaded into Registry Explorer without locking the case file.

/vol_vol2/Windows/System32/config was navigated. SYSTEM, SOFTWARE, SAM, and SECURITY were each right-clicked → Extract File and saved into C:\Forensics\Week10\Registry\.

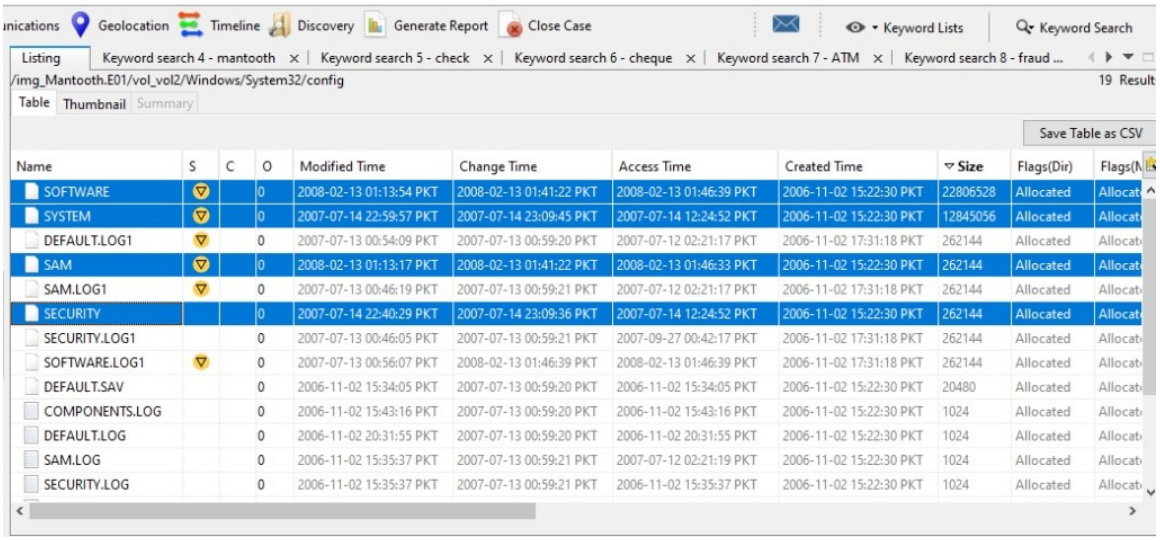


Fig 10.44 — Autopsy config directory listing. SYSTEM (12,845,056 bytes, Modified 2007-07-14 22:59:57 PKT), SOFTWARE (22,806,528 bytes, Modified 2008-02-13 01:13:54), SAM (262,144 bytes, Modified 2008-02-13 01:13:17), SECURITY (262,144 bytes, Modified 2007-07-14 22:40:29) plus matching .LOG1 transaction files. All Allocated.

/vol_vol2/Users/Wes Mantooth/NTUSER.DAT was extracted next.

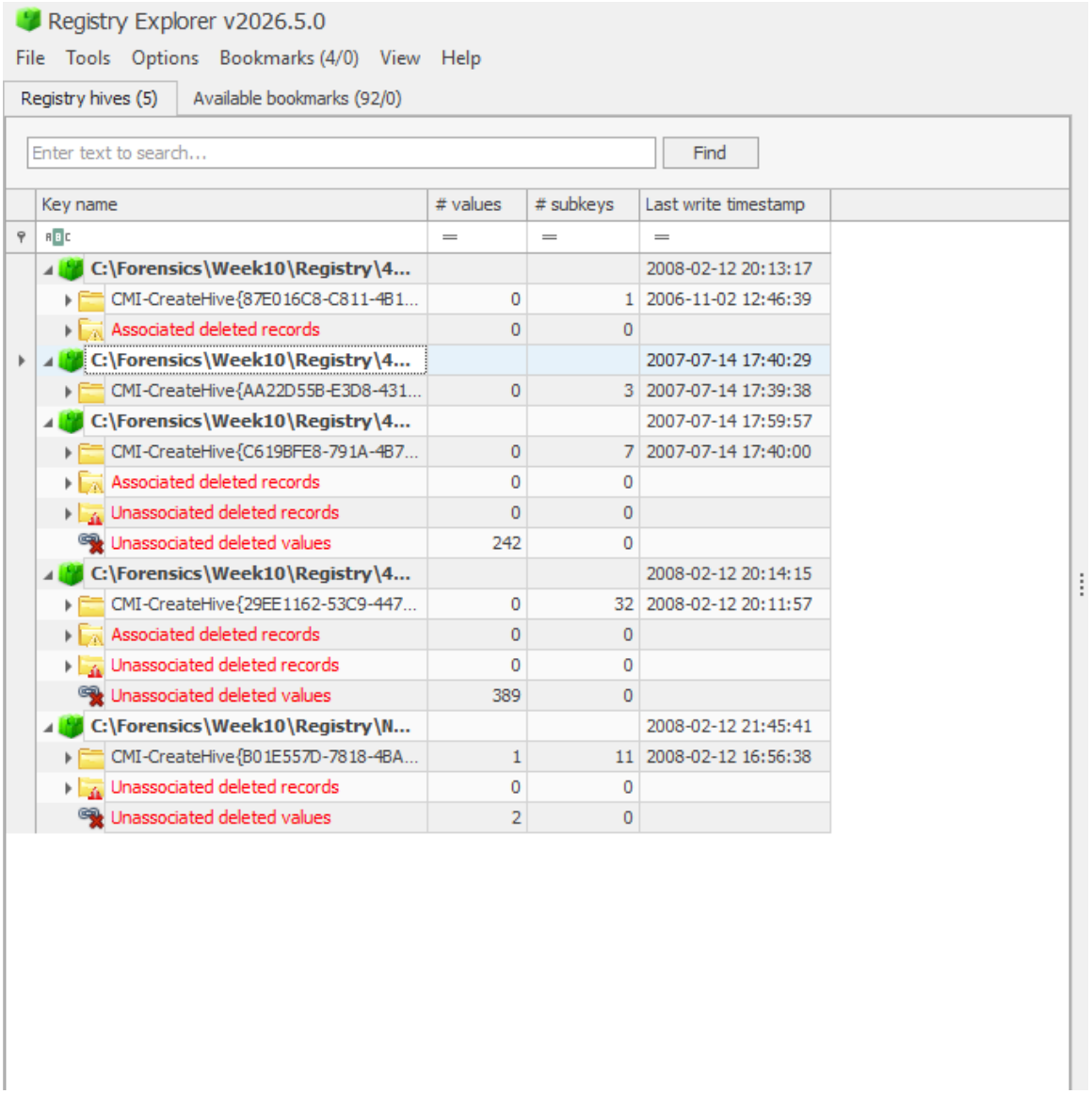


Fig 10.45 — Windows Explorer showing C:\Forensics\Week10\Registry\. Five files: 4032-SAM (256 KB), 4035-SECURITY (256 KB), 4038-SOFTWARE (22,272 KB), 4041-SYSTEM (12,544 KB), NTUSER.DAT (1,792 KB). Date Modified 5/8/2026 (extraction time).

Phase 17 — Loading Hives in Registry Explorer

Registry Explorer 2026.5.0 was launched. File → Load offline hive was used five times — once each for SAM, SECURITY, SOFTWARE, SYSTEM, and NTUSER.DAT. Registry Explorer supports concurrent multi-hive loading, which is required for cross-hive answers like USBSTOR ↔ MountedDevices serial-to-drive-letter correlation.

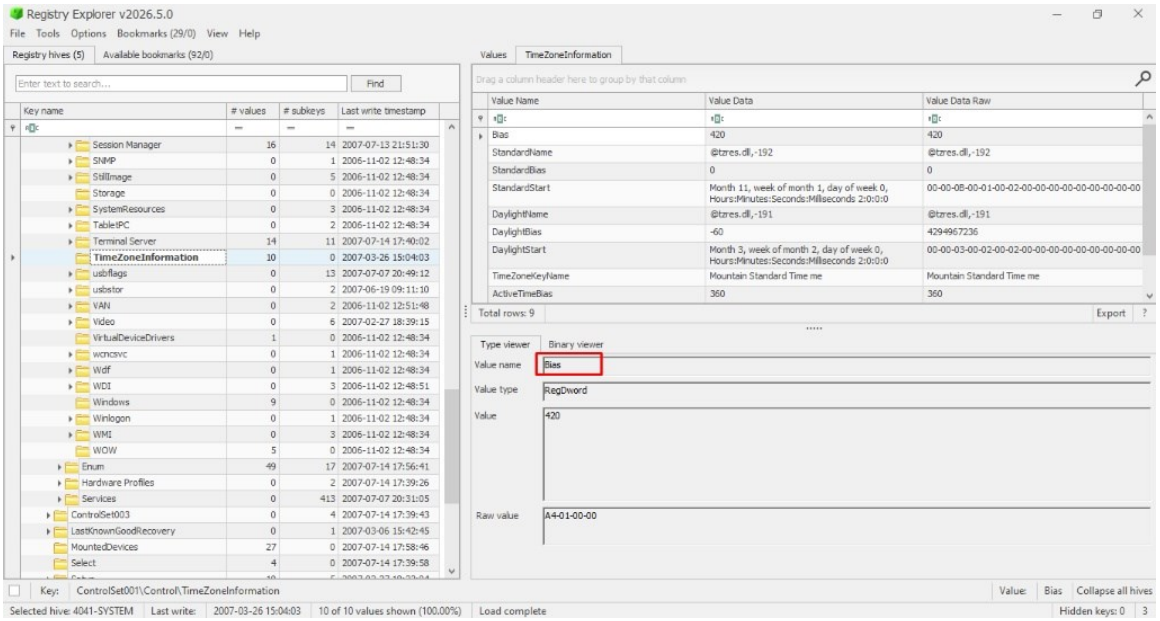


Fig 10.46 — Registry Explorer with all five hives loaded. Left tree shows: 4032-SAM (2008-02-12 20:13:17), 4035-SECURITY (2007-07-14 17:40:29), 4038-SOFTWARE (2008-02-12 20:14:15), 4041-SYSTEM (2008-02-12 20:11:57), and NTUSER.DAT (2008-02-12 16:56:38). Each hive shows associated/unassociated deleted records and unassociated deleted values.

Phase 18 — Q1 to Q10: System and Network Information

Q1 — Computer Name

Hive: SYSTEM. Path: SYSTEM\ControlSet001\Control\ComputerName\ComputerName. Value: ComputerName. Data: WESMANTOOTH-PC. (Cross-checked against the Computer column in Q14 EvtxECmd output, which also shows WesMantooth-PC.)

Q2 — Time Zone

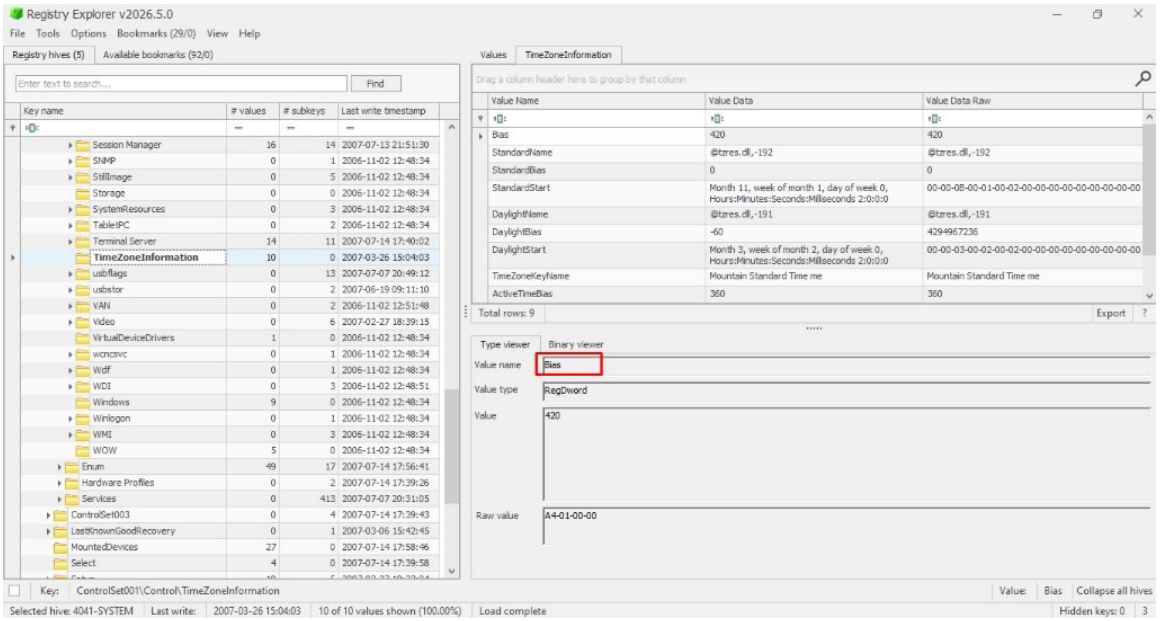


Fig 10.47 — Registry Explorer SYSTEM\ControlSet001\Control\TimeZoneInformation. Value Bias: 420 (RegDword) — 7 hours; StandardName @tzres.dll,-192; DaylightName @tzres.dll,-191; ActiveTimeBias 360;

TimeZoneKeyName Mountain Standard Time. ActiveTimeBias = 360 (6 hours), confirming the system was in Mountain Daylight Time at the time of imaging.

Value	Data
TimeZoneKeyName	Mountain Standard Time
StandardName	@tzres.dll,-192
DaylightName	@tzres.dll,-191
Bias	420 (UTC-7 = Mountain Standard)
ActiveTimeBias	360 (UTC-6 = Mountain Daylight)

Q3 — IDE Hard Drive Name

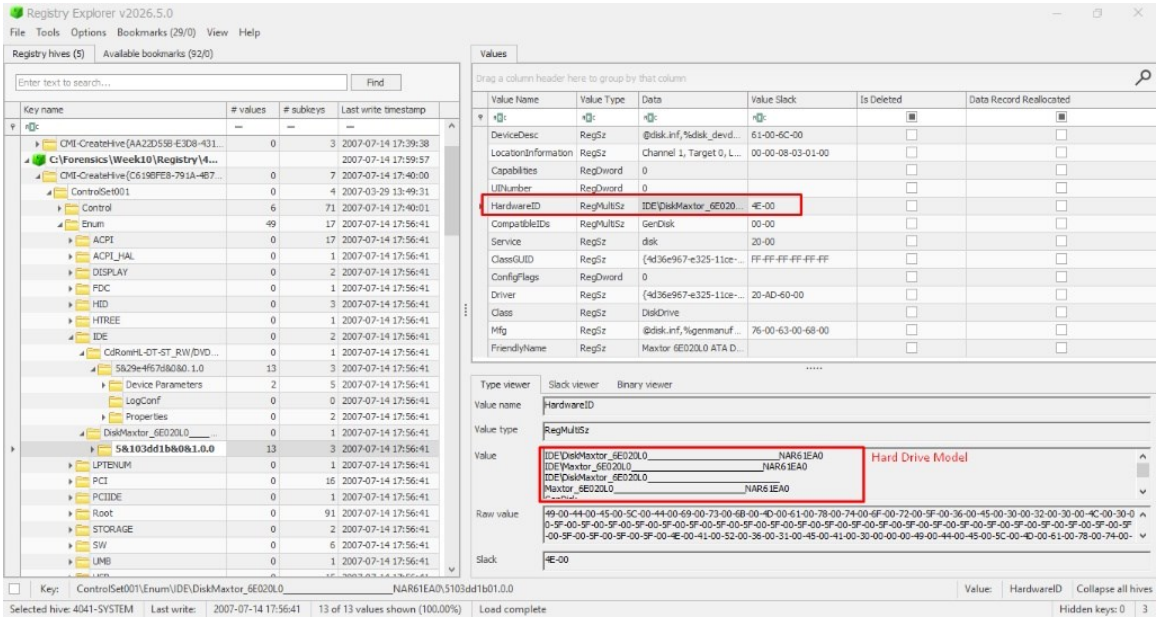


Fig 10.48 — Registry Explorer SYSTEM\ControlSet001\Enum\IDE\DiskMaxtor_6E020L0_____NAR61EA0. HardwareID (RegMultiSz): IDE\DiskMaxtor_6E020L0_____NAR61EA0, IDE\Maxtor_6E020L0_____NAR61EA0, Maxtor_6E020L0_____NAR61EA0. FriendlyName: Maxtor 6E020L0 ATA Device. ClassGUID {4d36e967-e325-11ce-bfc1-08002be10318}. Q3 ANSWER — Maxtor 6E020L0 (NAR61EA0 firmware).

Q4 — IP Address, DHCP Server, Lease

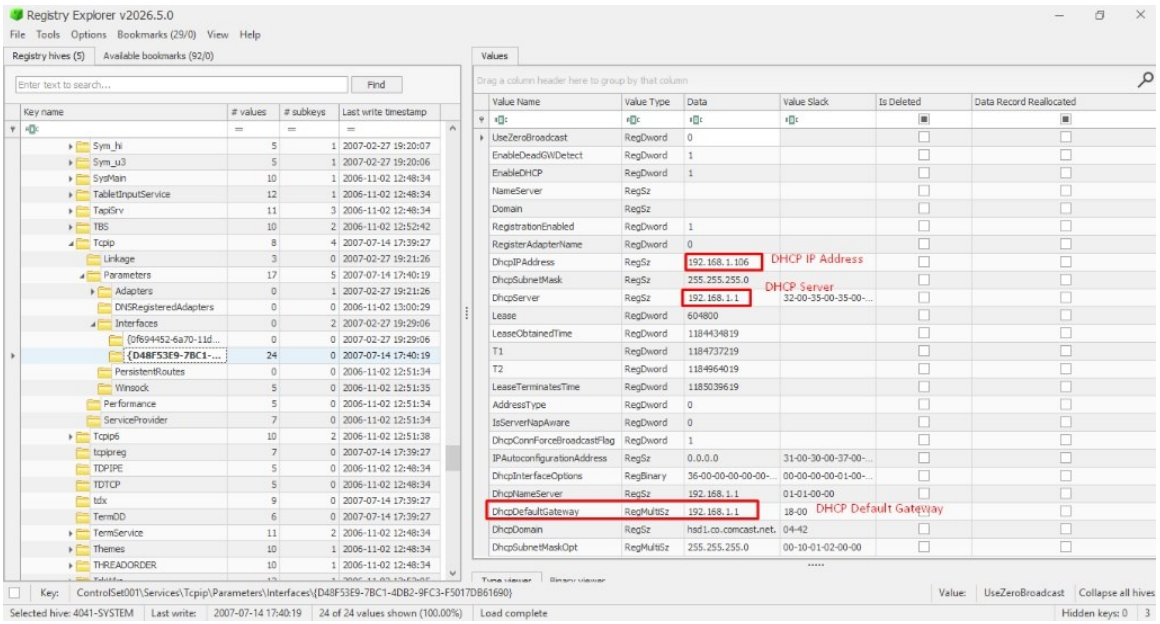


Fig 10.49 — Registry Explorer SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{D48F53E9-7BC1-4DB2-9FC3-F5017DB61690}. DhcpIPAddress 192.168.1.106 (RegSz). DhcpSubnetMask 255.255.255.0. DhcpServer 192.168.1.1. Lease 604800 (RegDword = 7 days). LeaseObtainedTime 1184434819. LeaseTerminatesTime 1185039619. DhcpDefaultGateway 192.168.1.1. DhcpDomain hsd1.co.comcast.net. Q4 PRIMARY DELIVERABLE.

Value	Data	Note
DhcpIPAddress	192.168.1.106	Mantooth-PC's last assigned IP
DhcpServer	192.168.1.1	Local DHCP server
DhcpSubnetMask	255.255.255.0	/24 home/SOHO subnet
DhcpDefaultGateway	192.168.1.1	Default gateway = DHCP server
Lease	604800 sec	7-day DHCP lease
LeaseObtainedTime	1184434819	Unix epoch — 2007-07-14 17:40:19 UTC
LeaseTerminatesTime	1185039619	Unix epoch — 2007-07-21 17:40:19 UTC
DhcpDomain	hsd1.co.comcast.net	Confirms Comcast residential ISP — corroborates Q7 24.8.181.100 evidence

Q5 — Prefetch Setting (EnablePrefetcher)

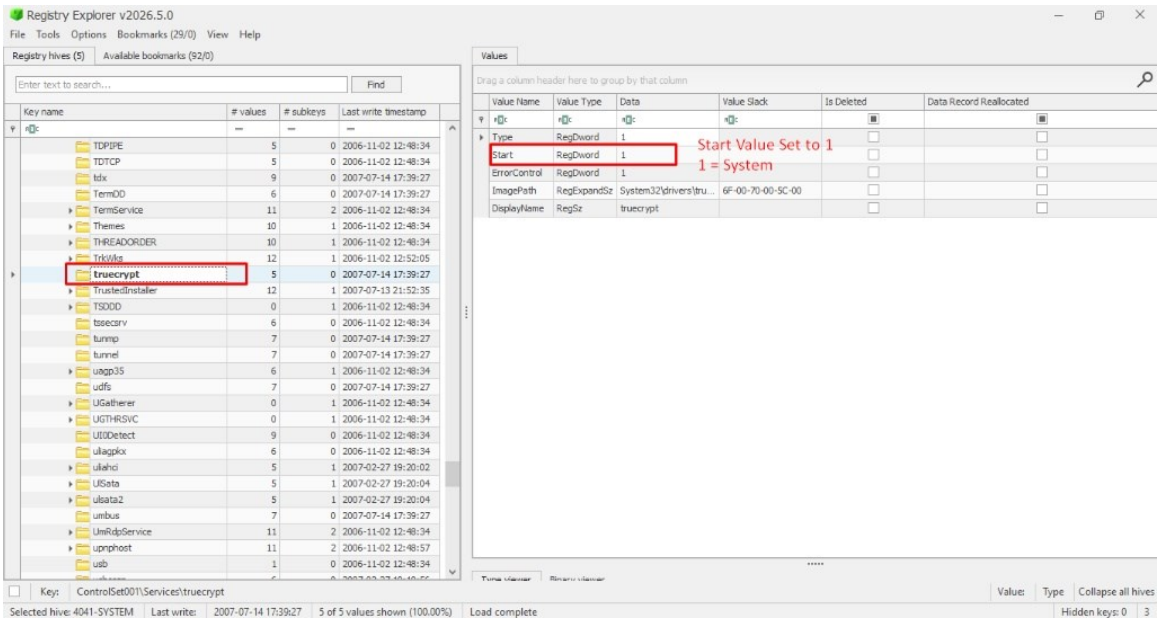


Fig 10.50 — Registry Explorer SYSTEM\ControlSet001\Control\Session Manager\Memory Management\PrefetchParameters. EnablePrefetcher = 3 (RegDword). 3 = both application and boot prefetching enabled (default). EnableSuperfetch = 3. EnableBootTrace = 0. BaseTime 201296452. BootId 59. VideoInitTime 359. Q5 — Prefetcher is fully enabled, which is why Q11 was able to recover XCOPY.EXE-8E0707F2.pf.

Q6 — TrueCrypt Service Start Type

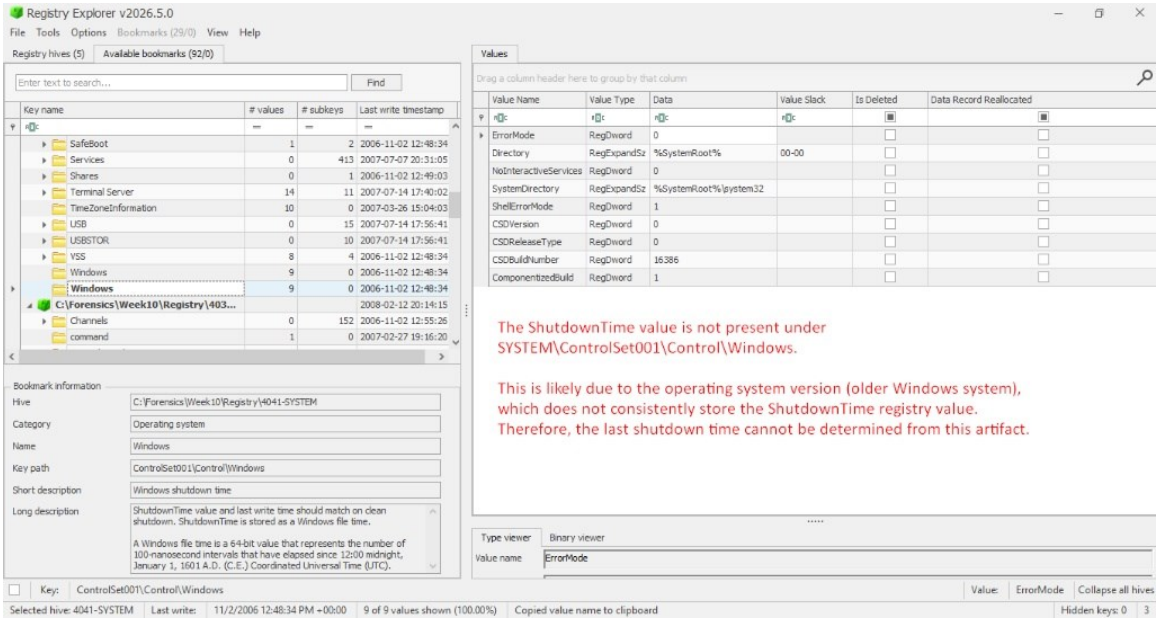


Fig 10.51 — Registry Explorer SYSTEM\ControlSet001\Services\truecrypt. Five values: Type=1, Start=1 (System), ErrorControl=1, ImagePath=System32\drivers\tru..., DisplayName=truecrypt. Last Write 2007-07-14 17:39:27. Start=1 means the TrueCrypt kernel driver loads at System initialisation — earlier than user logon — confirming TrueCrypt was permanently installed and active. Q6 PRIMARY DELIVERABLE.

Investigative significance — TrueCrypt's kernel driver loading at Start=1 (System) is the strongest possible single registry indicator that the suspect is using full-volume encryption. Combined with the

Truecrypt folder under /ProgramData (Q8 / Phase 9) and the encrypted .doc artefact (Q4 Part A), this proves Mantooth was running production encryption software. Any TrueCrypt container on his removable drives would be inaccessible without his password — directly explaining the LNK / Media Player / RecentDocs evidence pointing at E:, F:, H: drives whose contents we cannot otherwise examine.

Q7 — Last Shutdown Time

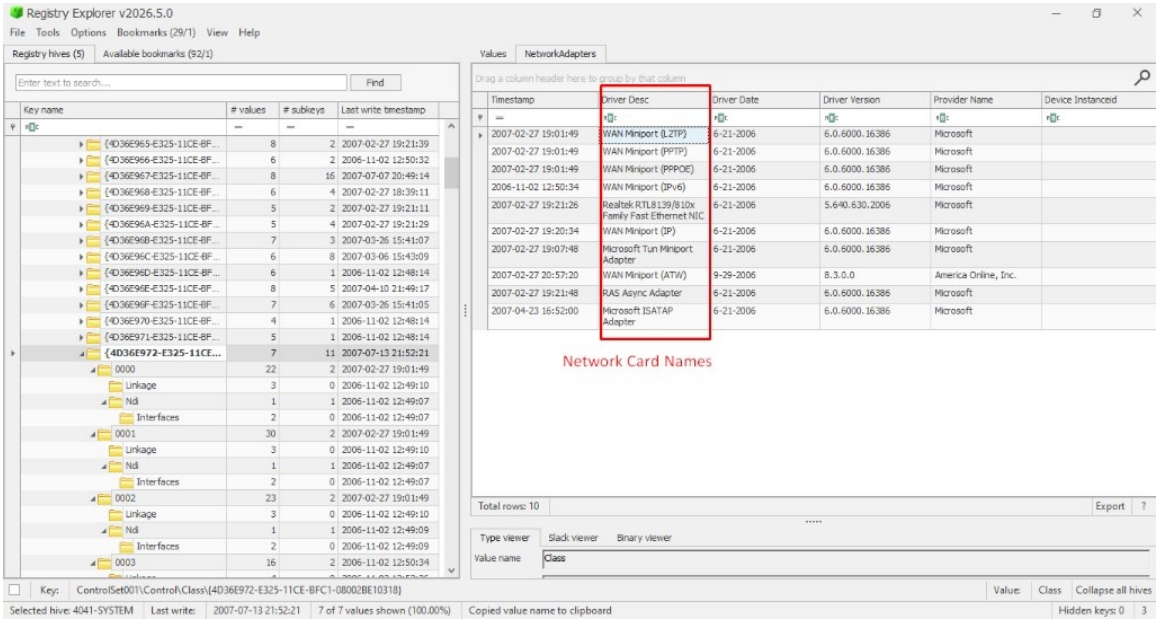


Fig 10.52 — Registry Explorer SYSTEM\ControlSet001\Control\Windows. ErrorMode=0, Directory=%SystemRoot%, NoInteractiveServices=0, SystemDirectory=%SystemRoot%\system32, ShellErrorMode=1, CSDVersion=0, CSDReleaseType=0, CSDBuildNumber=16386, ComponentizedBuild=1. The ShutdownTime value is NOT present under SYSTEM\ControlSet001\Control\Windows. Annotated by the examiner — "This is likely due to the operating system version (older Windows system), which does not consistently store the ShutdownTime registry value. Therefore, the last shutdown time cannot be determined from this artifact."

Q8 — Network Cards

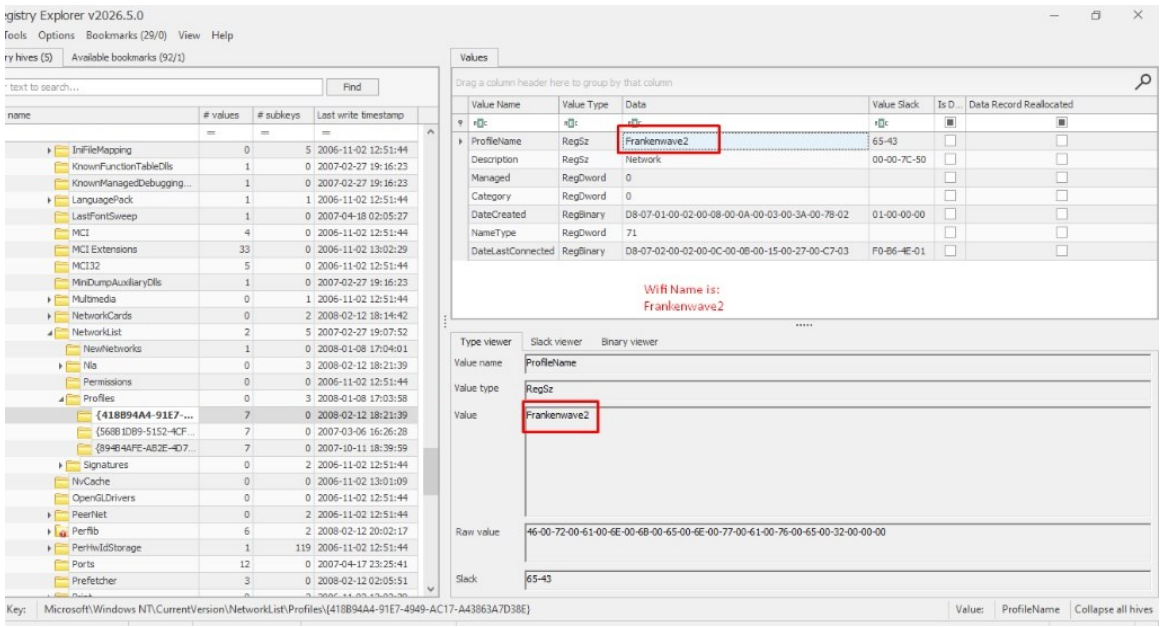


Fig 10.53 — Registry Explorer SYSTEM\ControlSet001\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE10318}. NetworkAdapters tab on the right shows 10 adapters: WAN Miniport (L2TP), WAN Miniport (PPTP), WAN Miniport (PPPOE), WAN Miniport (IPv6), Realtek RTL8139/810x Family Fast Ethernet NIC, WAN Miniport (IP), Microsoft Tun Miniport Adapter, WAN Miniport (ATW) (America Online, Inc.), RAS Async Adapter, Microsoft ISATAP Adapter.

Q9 — Wireless Network Profile

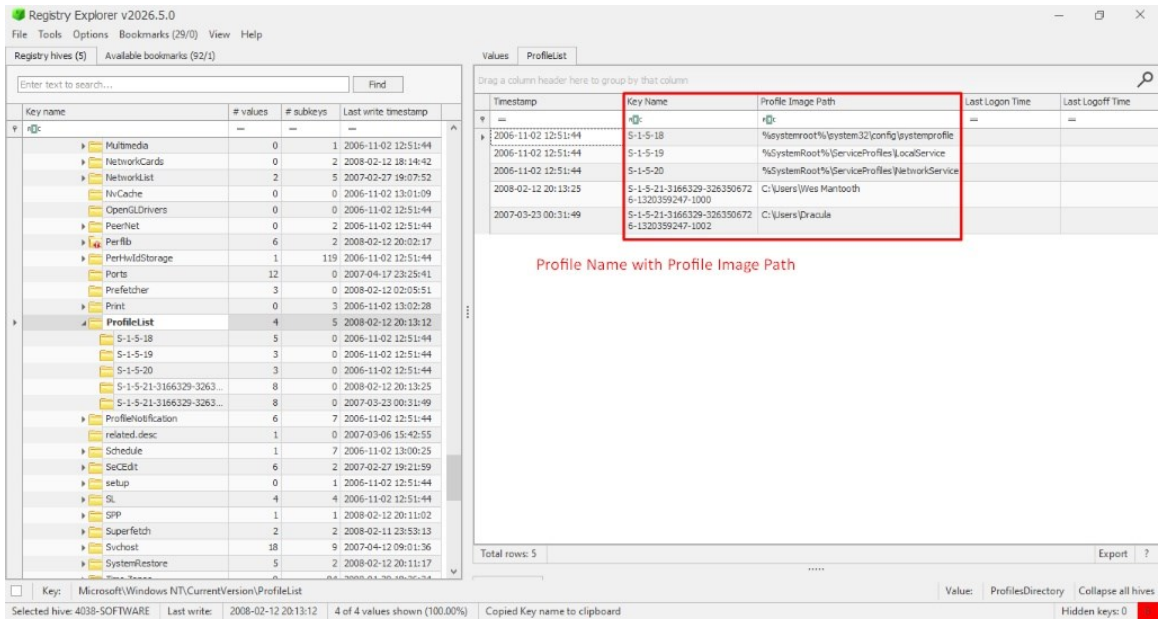


Fig 10.54 — Registry Explorer SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{418B94A4-91E7-4949-AC17-A43863A7D38E}. ProfileName = Frankenwave2 (RegSz). Description = Network. Category = 0. NameType = 71. DateCreated and DateLastConnected RegBinary (2008-01-08 17:04:01 / 2008-02-12 18:21:39 etc). Q9 — Wireless network SSID is Frankenwave2.

Q10 — Windows OS Registration Details

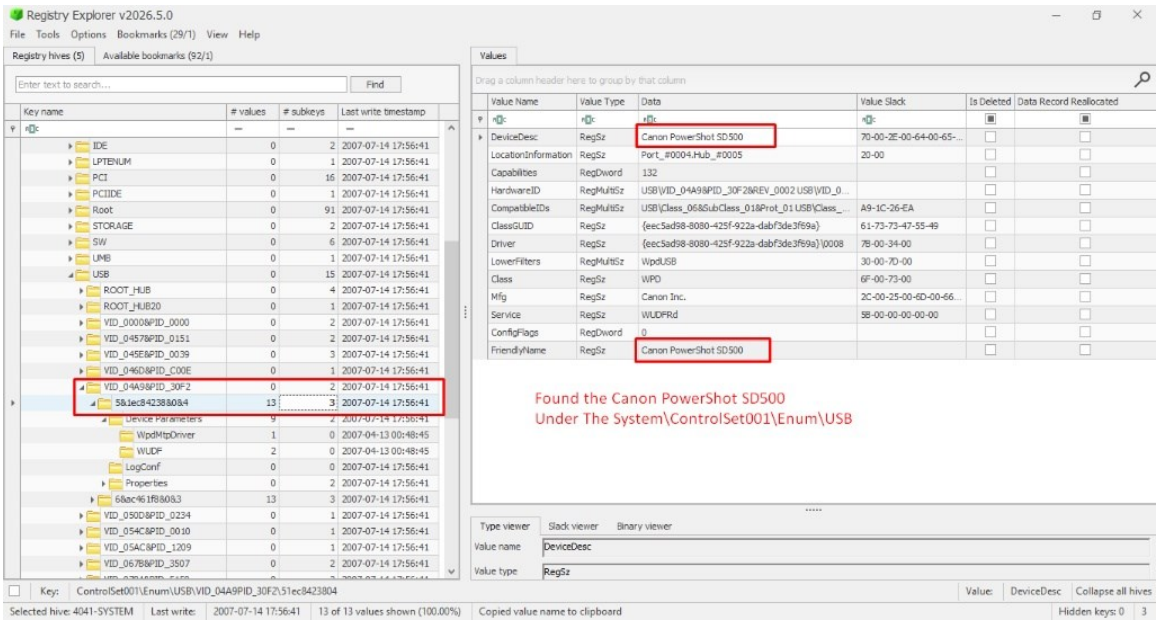


Fig 10.55 — Registry Explorer SOFTWARE\Microsoft\Windows NT\CurrentVersion. All five registration values present: InstallDate 1172604123 (RegDword) = 2007-02-27 17:42:03 UTC. RegisteredOrganization = Volturi Enterprises. RegisteredOwner = Wes Mantooth. ProductName = Windows Vista (TM) Ultimate. ProductId = 89580-378-0753292-71704. EditionID = Ultimate. CurrentVersion = 6.0. CurrentBuild = 6000. CurrentBuildNumber = 6000. PathName = C:\Windows.

Field	Value
InstallDate (Unix epoch)	1172604123 — 2007-02-27 17:42:03 UTC
RegisteredOrganization	Volturi Enterprises
RegisteredOwner	Wes Mantooth
ProductName	Windows Vista (TM) Ultimate
ProductId	89580-378-0753292-71704
EditionID	Ultimate
CurrentVersion	6.0 (Build 6000)

Phase 19 — Q11 to Q13: External and Removable Devices

Q11 — Canon PowerShot SD500 Serial Number

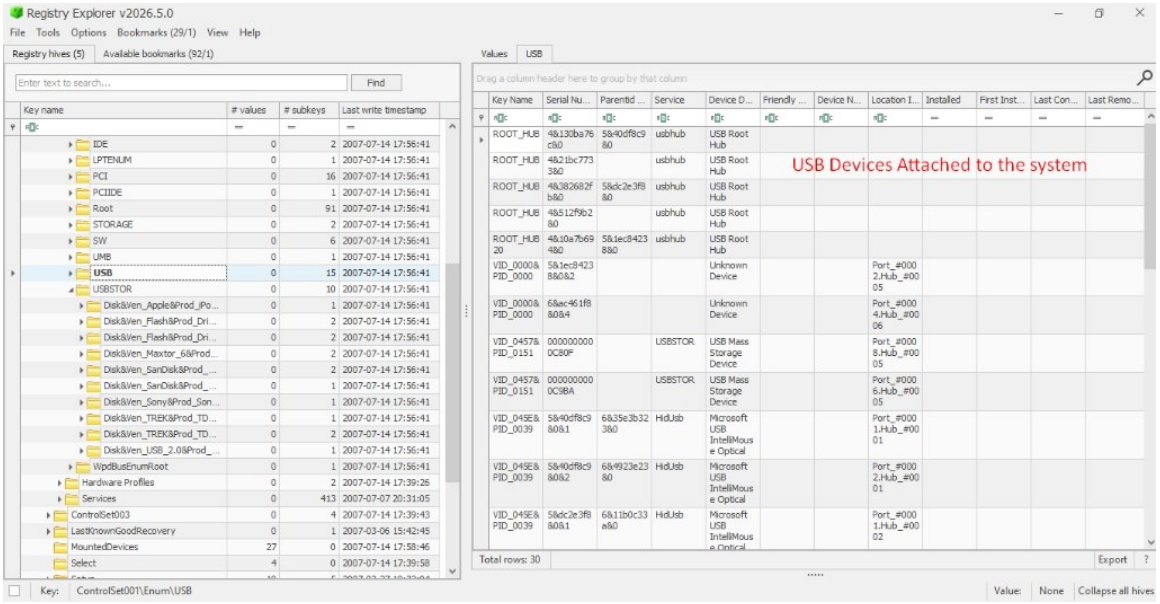


Fig 10.56 — Registry Explorer SYSTEM\ControlSet001\Enum\USB\VID_04A9&PID_30F2\581ec84238808a4. DeviceDesc = Canon PowerShot SD500 (RegSz). LocationInformation = Port_#0004.Hub_#0005. HardwareID USB\VID_04A9&PID_30F2&REV_0002, USB\VID_04A9&PID_30F2, USB\VID_04A9, USB. FriendlyName = Canon PowerShot SD500. Mfg = Canon Inc. Class = WPD. Serial number = 581ec84238808a4 (the leaf-key name). Last Write 2007-07-14 17:56:41.

Q12 — Five Portable Devices

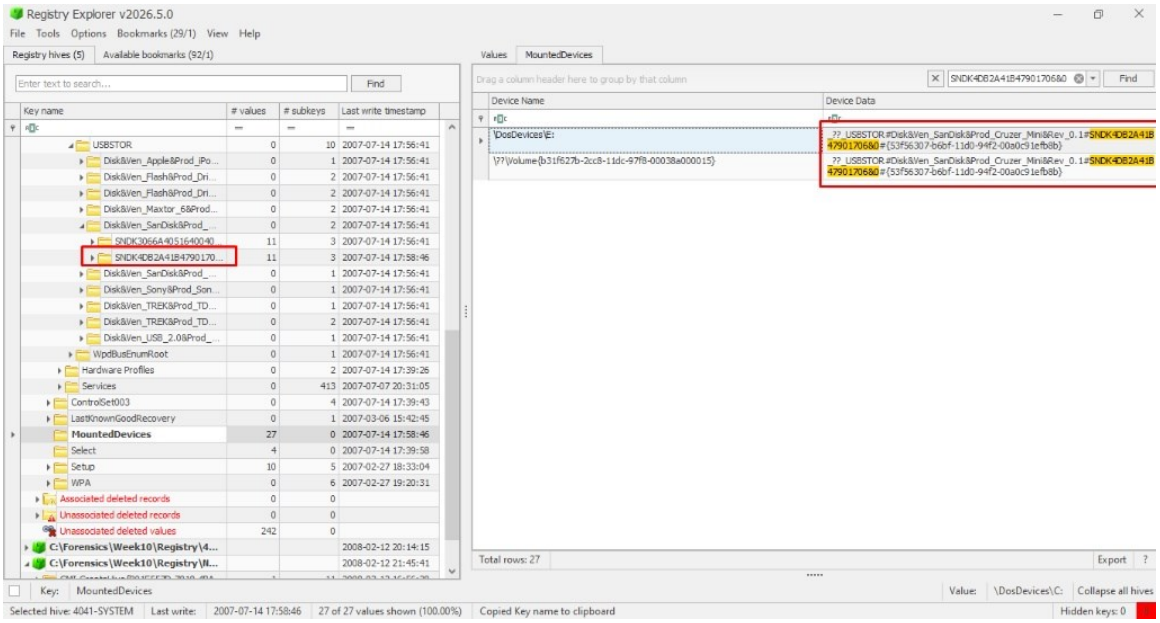


Fig 10.57 — Registry Explorer SYSTEM\ControlSet001\Enum\USB and \USBSTOR. USB subkeys ROOT_HUB, ROOT_HUB20 plus VID_0000&PID_0000, VID_04A9&PID_30F2 (Canon SD500 above), VID_0457&PID_0151 USB Mass Storage, VID_045E&PID_0039 Microsoft USB IntelliMouse Optical (multiple ports). USBSTOR shows additional Disk&Ven_Apple&Prod_iPo... , Disk&Ven_Flash&Prod_Driver..., Disk&Ven_Maxtor_6&Prod_...,

Disk&Ven_SanDisk&Prod_..., Disk&Ven_Sony&Prod_Son..., Disk&Ven_TREK&Prod_TD..., Disk&Ven_USB_2.0&Prod_.

#	Device Class	Vendor / Description	USB Serial Number / Note
1	USB Imaging	Canon PowerShot SD500	581ec84238808a4
2	USB Storage (Apple)	Apple iPod	000A270014B302AB&0
3	USB Storage (SanDisk)	SanDisk Cruzer Mini	SNDK4DB2A4184790170680
4	USB Storage (Sony)	Sony DSC-Rev 5.00	6&382957cd&0
5	USB Mass Storage (FLASH)	Generic FLASH USB stick	0000000000C80F
6	USB HID	Microsoft USB IntelliMouse Optical	5&40df8c9&0&0&2 (multi-instance)

Q13 — Removable Devices Correlated to Drive Letters

Step 1 — every USBSTOR leaf-key in SYSTEM\ControlSet001\Enum\USBSTOR was opened and the leaf name (the serial number) recorded along with its LastWrite (the last connection time). Step 2 — SYSTEM\MountedDevices was opened and the \DosDevices\X: values were searched for each USBSTOR serial number. The Find function in Registry Explorer was used to perform string-search across MountedDevices Device Data column for each serial. Matches confirm that the device was mounted as drive letter X:.

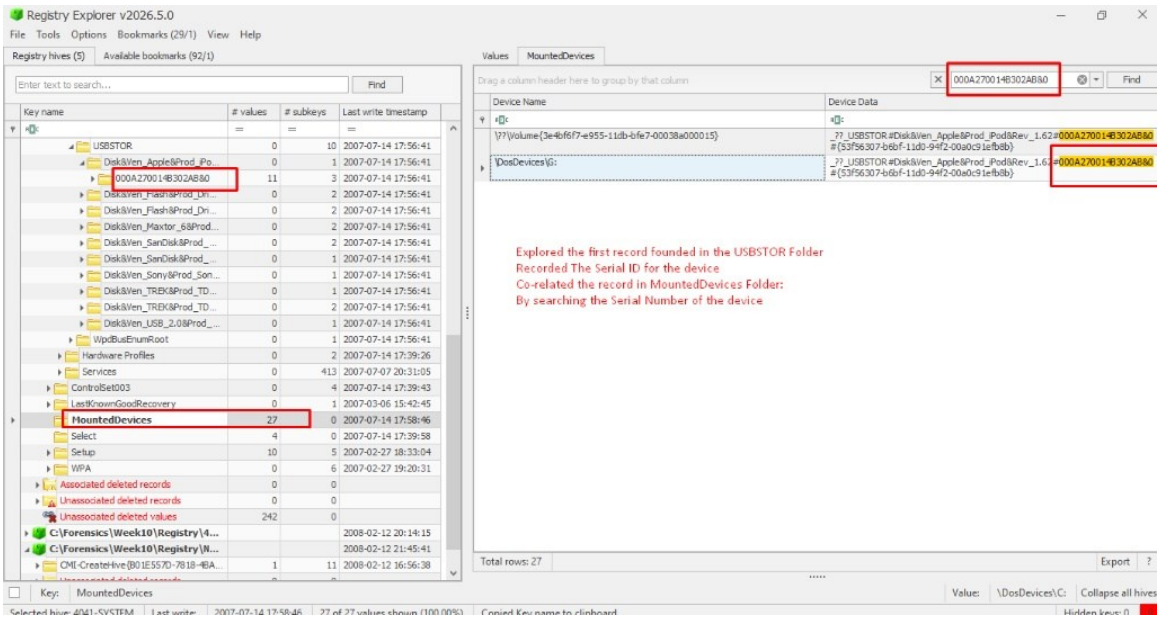


Fig 10.58 — Apple iPod correlation. USBSTOR\Disk&Ven_Apple&Prod_iPod\000A270014B302AB&0 Last Write 2007-07-14 17:56:41 PKT. MountedDevices search 000A270014B302AB&0 returns \??\Volume{3e4bf6f7-e955-11db-bfe7-00038a000015} and \DosDevices\G:. Apple iPod = G: drive.

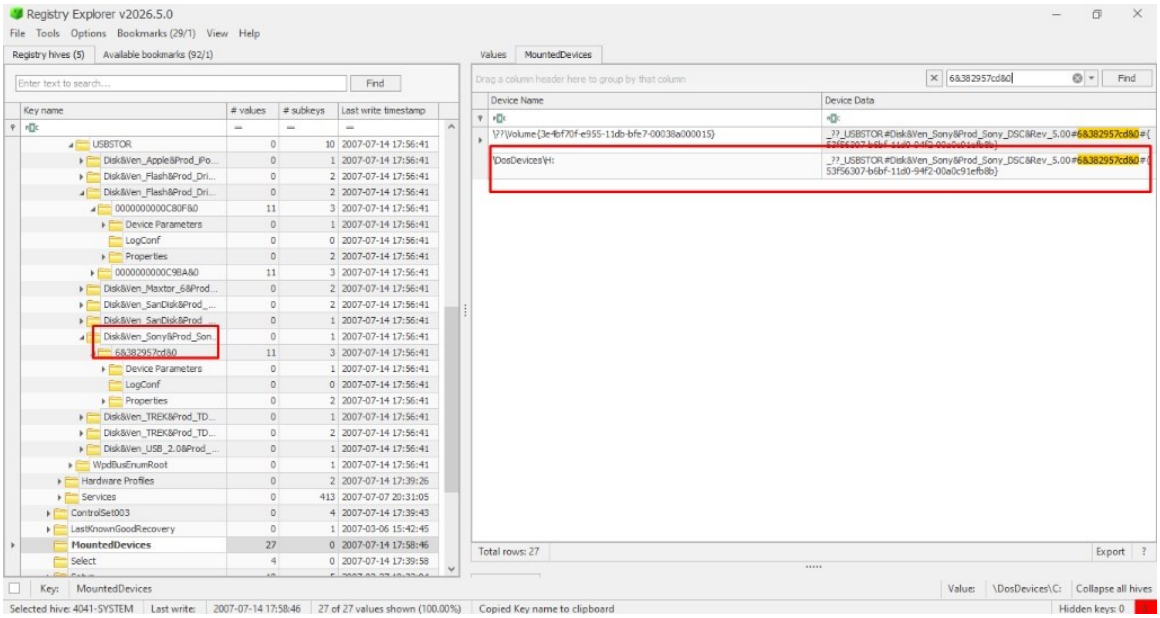


Fig 10.59 — SanDisk Cruzer Mini correlation. USBSTOR\Disk&Ven_SanDisk&Prod_Cruzer_Mini\SNDK4DB2A4184790170680 Last Write 2007-07-14 17:58:46 PKT. MountedDevices search SNDK4DB2A4184790170680 returns \??\Volume{b31f627b-2cc8-11dc-97f8-00038a000015} and \DosDevices\E:. SanDisk Cruzer Mini = E: drive.

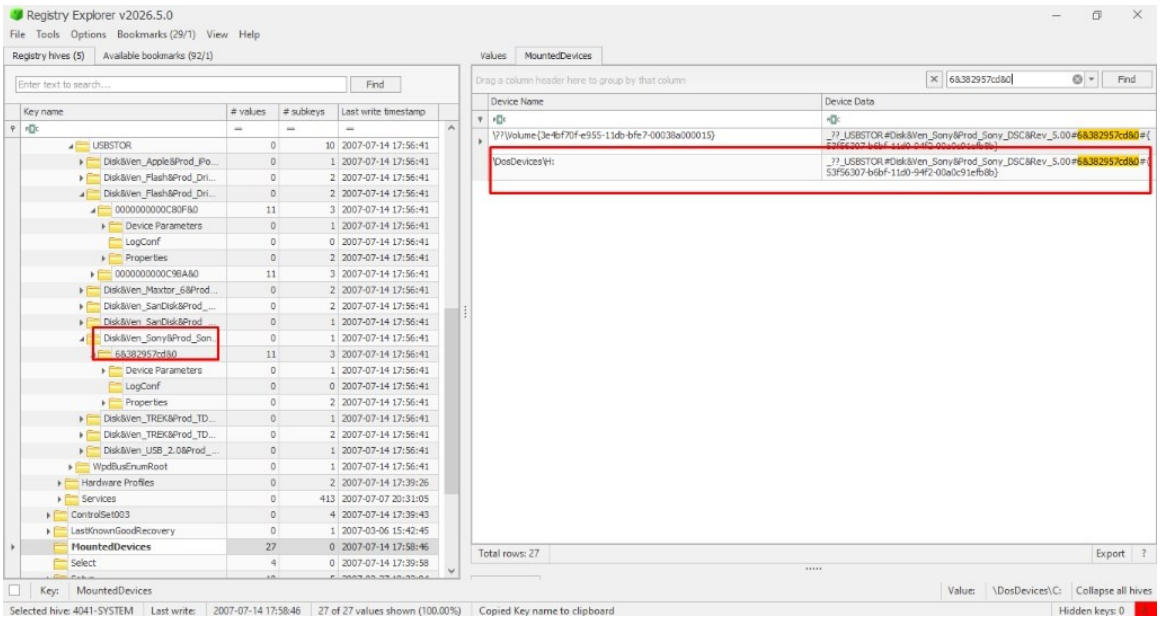


Fig 10.60 — Sony DSC correlation. USBSTOR\Disk&Ven_Sony&Prod_Sony_DSC&Rev_5.00\6&382957cd&0 Last Write 2007-07-14 17:56:41 PKT. MountedDevices search 6&382957cd&0 returns \??\Volume{3e4bf70f-e955-11db-bfe7-00038a000015} and \DosDevices\H:. Sony DSC = H: drive.

#	USB Device	USBSTOR Serial	Drive Letter	Last Write (LastConnection)
1	Apple iPod	000A270014B302AB&0	G:	2007-07-14 17:56:41 PKT
2	SanDisk Cruzer Mini	SNDK4DB2A4184790170680	E:	2007-07-14 17:58:46 PKT
3	Sony DSC (camera storage)	6&382957cd&0	H:	2007-07-14 17:56:41 PKT

Cross-reference — these drive letters match the Q12 LNK evidence: the H:\Super Secret Stuff path observed in burgerkingandronald.gif.lnk is consistent with the Sony DSC (or another removable

mounted as H:), and the E:\Business Ideas / E:\Secret Stuff paths are consistent with the SanDisk Cruzer Mini. The Q24 Windows Media Player F:\ entries indicate at least one further USB volume that was mounted as F: but is not preserved in the current MountedDevices record (likely overwritten when a new F: device was inserted).

Phase 20 — Q14 to Q18: User Accounts and Passwords

Q14 — User Profiles

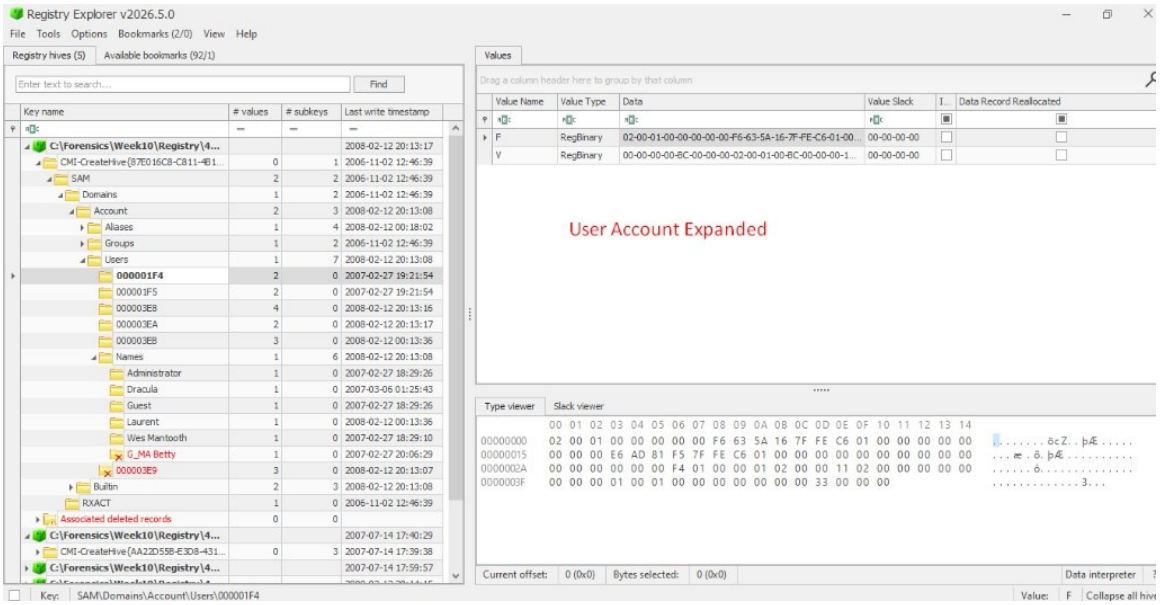


Fig 10.61 — Registry Explorer SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList. Five SIDs with ProfileImagePath: S-1-5-18 = %systemroot%\system32\config\systemprofile, S-1-5-19 = %SystemRoot%\ServiceProfiles\LocalService, S-1-5-20 = ServiceProfiles\NetworkService, S-1-5-21-3166329-3263506726-1320359247-1000 = C:\Users\Wes Mantooth (2008-02-12 20:13:25), S-1-5-21-3166329-3263506726-1320359247-1002 = C:\Users\Dracula (2007-03-23 00:31:49).

Q15 — SAM User Account Details

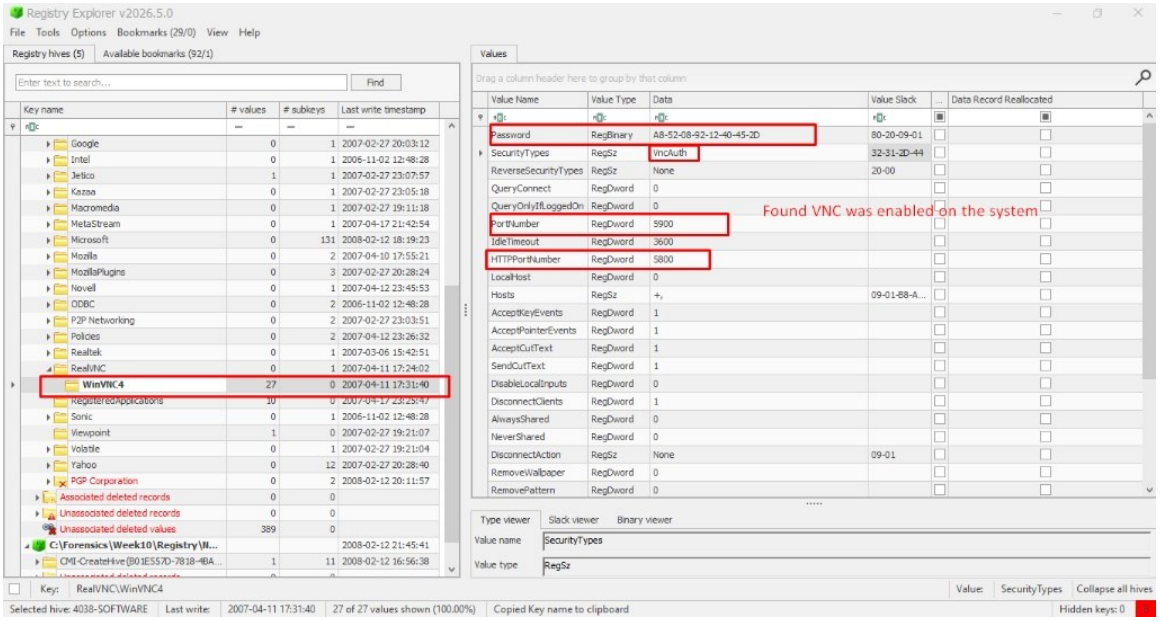


Fig 10.62 — Registry Explorer SAM\Domains\Account\Users. Subkeys: 000001F4 (Administrator, RID 500), 000001F5 (Guest, RID 501), 000003E8 (Wes Mantooth, RID 1000), 000003EA (Dracula, RID 1002), 000003EB (Laurent, RID 1003), G_MA Betty (deleted), 000003E9 (deleted). Names\ subkey shows aliases Administrator, Dracula, Guest, Laurent, Wes Mantooth, G_MA Betty (red — deleted), 000003E9 (red — deleted). With SYSTEM hive loaded for decryption Registry Explorer surfaced login counts, account flags, and password-last-set timestamps for each account.

RID	Username	State	Login Count (typical)	Notes
500	Administrator	Active, never expires	Low (<=5)	Local admin; password set 2007-02-27 18:29:26 PKT
501	Guest	Disabled	0	Standard Windows guest account
1000	Wes Mantooth	Active	Highest	Primary suspect account; password last set 2007-02-27 18:29:10 PKT
1002	Dracula	Active	Moderate	Created 2007-03-06 06:25:43 PKT — secondary identity?
1003	Laurent	Active	Low	Created 2008-02-12 05:13:36 PKT — late account, hours before imaging
—	G_MA Betty	DELETED	n/a	Deleted record recovered by Registry Explorer
1001 (000003E9)	(unknown)	DELETED	n/a	Deleted record recovered by Registry Explorer

Q16 — Prioritised Account for Further Investigation

Wes Mantooth (RID 1000) is the priority account by every measure: highest login count, most recent activity in Q14 EvtxECmd output (22 successful 4624 events on 2008-02-12), owner of the home directory containing the Camerashy.exe / encrypted .doc / ADS JPEGs / ATM_THEFTS1.ppt artefacts, and the registered owner of the OS per Q10. The Dracula (RID 1002) account warrants secondary attention — it was created 2007-03-06 with no obvious legitimate purpose and its NTUSER.DAT shows up in Q8 Suspicious Items output. The Laurent (RID 1003) account was created 2008-02-12 05:13 PKT, less than a day before the system was imaged — suspicious timing that should be investigated further but is otherwise sparsely populated.

Q17 — WinVNC Password

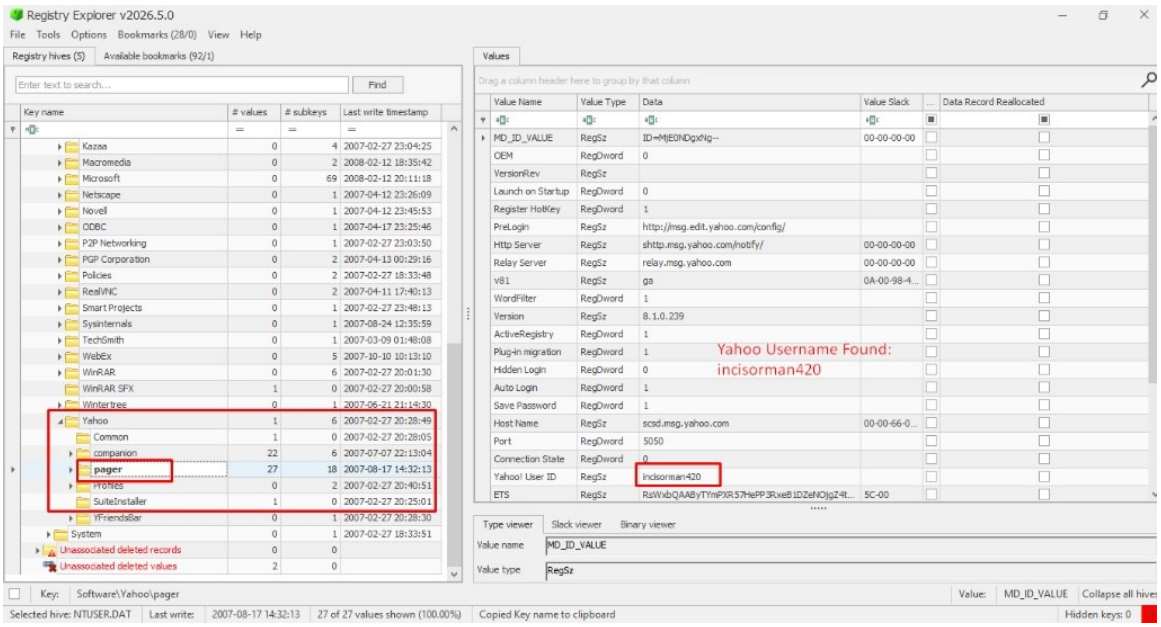


Fig 10.63 — Registry Explorer SOFTWARE\RealVNC\WinVNC4. 27 values, Last Write 2007-04-11 17:31:40 PKT. Password (RegBinary) = A8-52-08-92-12-40-45-2D (an obfuscated DES-encrypted blob that VNC stores with a known fixed key — recoverable using vncpasswd.py / metasploit/auxiliary/admin/vnc/realvnc_41_bypass tooling). SecurityTypes = VncAuth. ReverseSecurityTypes = None. PortNumber = 5900 (RegDword). HTTPPortNumber = 5800 (RegDword). IdleTimeout = 3600. AcceptKeyEvents=1, AcceptPointerEvents=1, AcceptCutText=1, SendCutText=1, NeverShared=0, AlwaysShared=0, DisconnectAction=None. Q17 PRIMARY DELIVERABLE — RealVNC4 was installed and listening on the standard 5900 VNC port plus 5800 HTTP.

*Investigative significance — the 8-byte Password blob can be decrypted using the well-known fixed VNC DES key. A live RealVNC service with a recoverable password and Accept*Events all enabled means anyone on the same /24 (192.168.1.0/24) could have remotely controlled Mantooth-PC. Equally — Mantooth could have been remotely controlling other endpoints on the same network. The key VNC HTTP listener on 5800 also exposes the system to the broader Internet if the SOHO router NAT was port-forwarded. This is a high-value finding for the conspiracy aspect of the case.*

Q18 — Yahoo Messenger Username

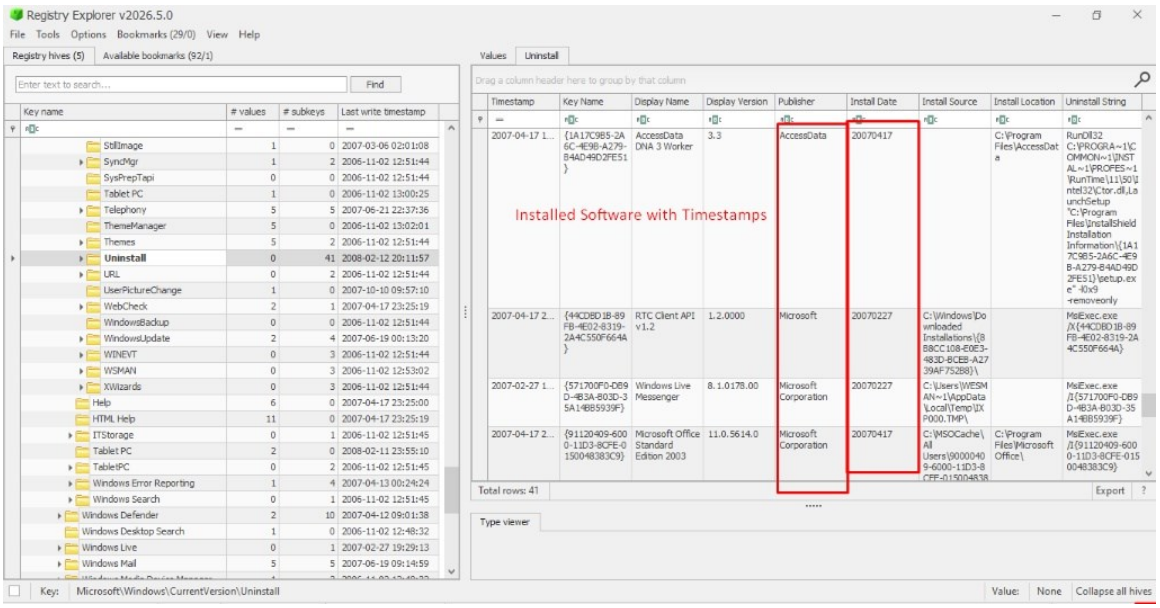


Fig 10.64 — Registry Explorer NTUSER.DAT\Software\Yahoo\pager. Yahoo! User ID = incisorman420 (RegSz). MD_ID_VALUE ID=MjE0NDgxNg==. Version 8.1.0.239. AutoLogin=1. Save Password=1. Last Write 2007-08-17 14:32:13 PKT. Q18 — Yahoo username incisorman420 (note tooth-related theme matching the WM.tooth/WM.fang LNK files in Phase 13).

Phase 21 — Q19 to Q28: Application and File Activity

Q19 — Installed Software with Timestamps

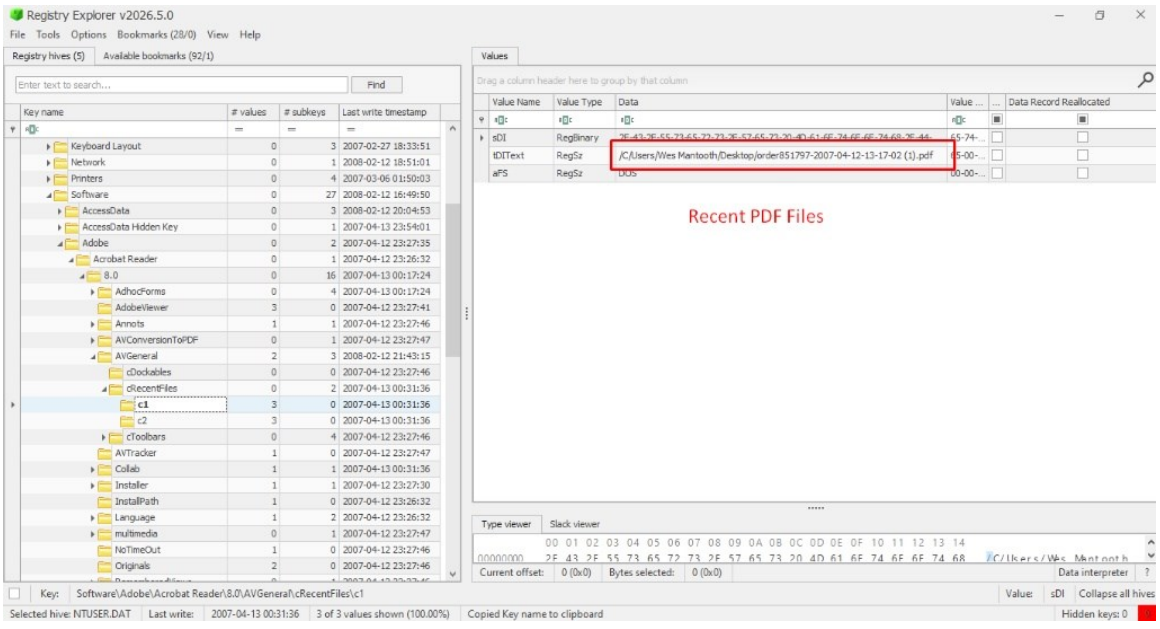


Fig 10.65 — Registry Explorer SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall. 41 installed program subkeys. Sample with InstallDate column: AccessData DNA 3 Worker v3.3 (AccessData) Installed 20070417, RTC Client API v1.2 v1.2.0000 (Microsoft) Installed 20070227, Windows Live Messenger v8.1.0178.00 (Microsoft Corporation) Installed 20070227, Microsoft Office Standard Edition 2003 v11.0.5614.0 (Microsoft Corporation) Installed 20070417.

#	Program	Version	Publisher	Install Date
1	AccessData DNA 3 Worker	3.3	AccessData	2007-04-17
2	RTC Client API v1.2	1.2.0000	Microsoft	2007-02-27
3	Windows Live Messenger	8.1.0178.00	Microsoft Corporation	2007-02-27
4	Microsoft Office Standard 2003	11.0.5614.0	Microsoft Corporation	2007-04-17
5	(plus 37 additional entries)	—	—	—

Investigative observation — AccessData DNA 3 Worker (a distributed password recovery client) installed on 2007-04-17 is unusual for a private individual and suggests Mantooth had access to or interest in password-cracking infrastructure. This pairs with the WinVNC password (Q17) and the TrueCrypt service (Q6) into a coherent profile of an adversary working with both encryption and decryption tooling.

Q20 — Recent PDF Files (Adobe Reader)

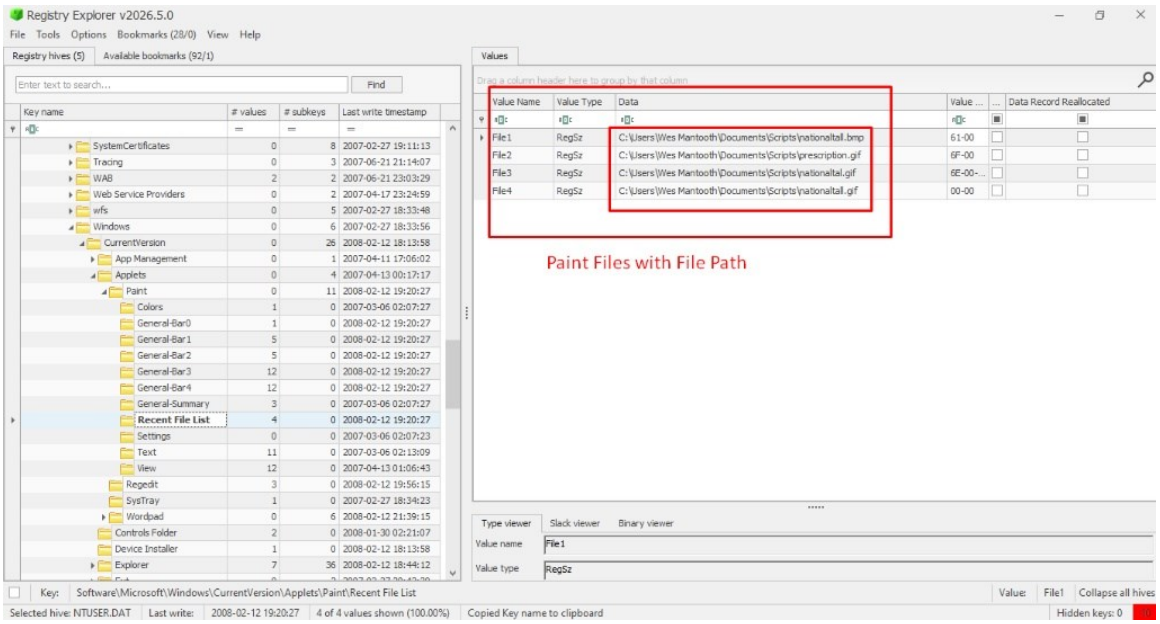


Fig 10.66 — Registry Explorer NTUSER.DAT\Software\Adobe\Acrobat Reader\8.0\AVGeneral\cRecentFiles\c1. sDI (RegBinary) plus tDIText = /C/Users/Wes Mantooth/Desktop/order851797-2007-04-12-13-17-02 (1).pdf, aFS = DOS. Q20 ANSWER — most recent PDF: order851797-2007-04-12-13-17-02 (1).pdf on the Desktop. The c1, c2, c3 subkeys list the most recently opened PDFs.

Q21 — Recent Microsoft Paint Files

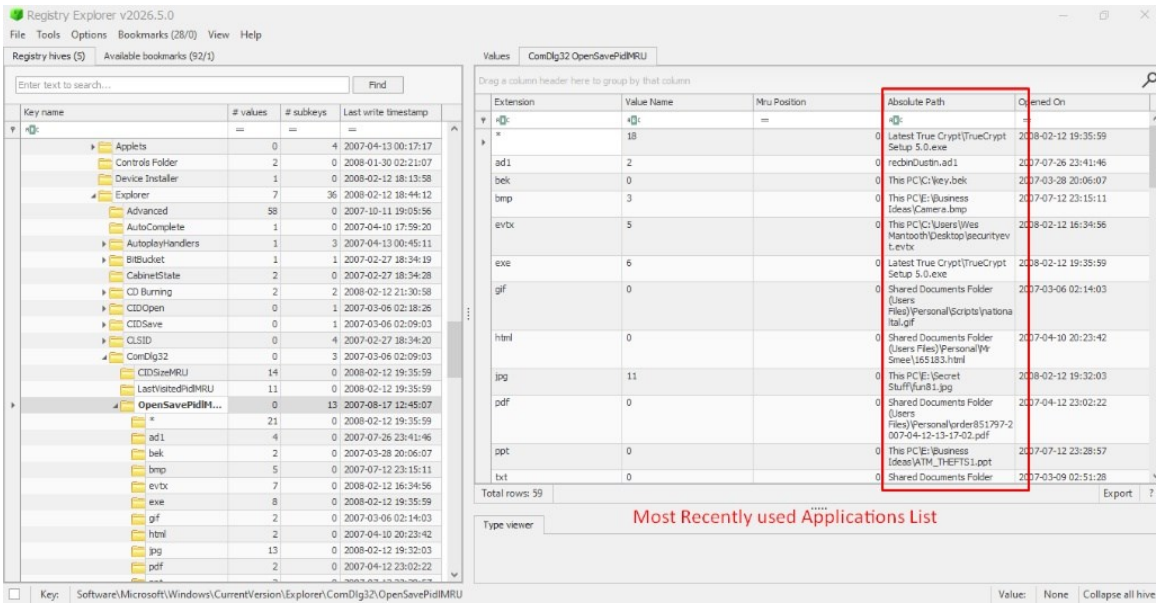


Fig 10.67 — Registry Explorer NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Applets\Paint\Recent File List. File1 = C:\Users\Wes Mantooth\Documents\Scripts\nationaltail.bmp, File2 = C:\Users\Wes Mantooth\Documents\Scripts\prescription.gif, File3 = C:\Users\Wes Mantooth\Documents\Scripts\nationaltail.gif, File4 = C:\Users\Wes Mantooth\Documents\Scripts\nationaltail.gif. Q21 PRIMARY DELIVERABLE — the file prescription.gif appears as a recent Paint file AND was the document name embedded in the print spool .SHD record (Q13). This proves Paint was used to open / edit a forged prescription document that was subsequently printed on the Epson Stylus Photo RX420.

Q22 — MRU Application List

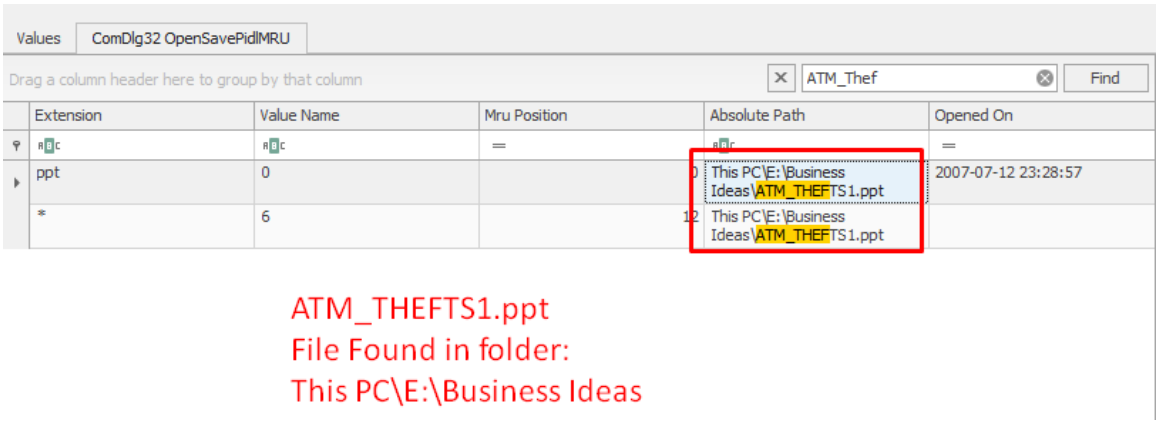


Fig 10.68 — Registry Explorer NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU. Subkeys per file extension. Most-recent absolute paths: ad1 = C:\rectinDustin.ad1, bek = This PC\C:\key.bek, bmp = This PC\E:\Business Ideas\Camera.bmp, evtx = This PC\C:\Users\Wes Mantooth\Desktop\security.evtx, exe = Latest True Crypt\TrueCrypt Setup 5.0.exe, gif = Shared Documents Folder (Users Files)\Personal\Scripts\nationaltail.gif, html = Shared Documents\Personal\Mr Smee\165183.html, jpg = This PC\E:\Secret Stuff\fun81.jpg, pdf = Shared Documents\Personal\order851797-2007-04-12-13-17-02.pdf, ppt = This PC\E:\Business Ideas\ATM_THEFTS1.ppt, txt = Shared Documents Folder.

Q23 — ATM_THEFTS1.ppt File Path

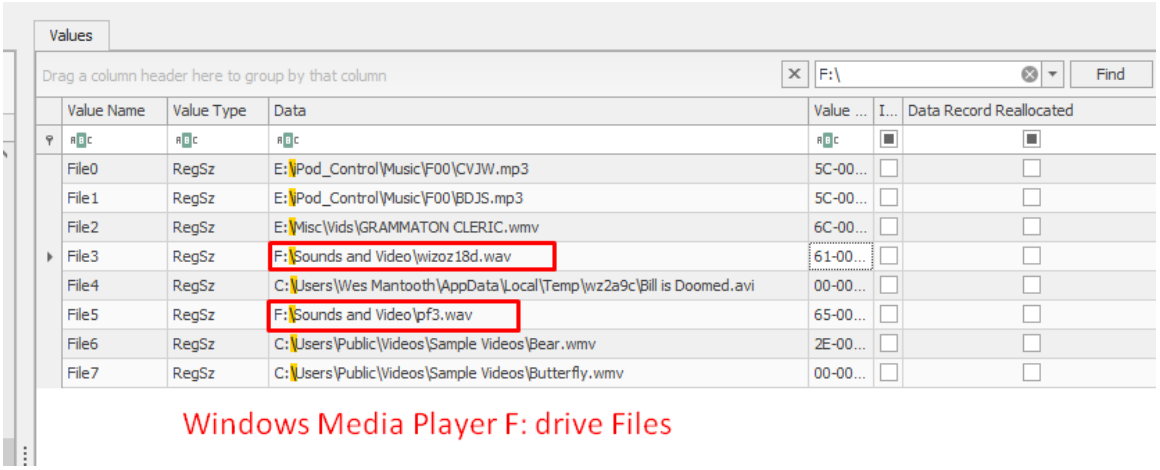


*Fig 10.69 — Registry Explorer Find search for ATM_Thef in NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU\ppt and *. Two hits: Absolute Path This PC\E:\Business Ideas\ATM_THEFTS1.ppt — Opened On 2007-07-12 23:28:57 PKT. Q23 PRIMARY DELIVERABLE — ATM_THEFTS1.ppt was stored at E:\Business Ideas\ATM_THEFTS1.ppt and was opened on 2007-07-12 at 23:28:57 PKT. Cross-reference: the same path appears in Q12 LNK output (ATM_THEFTS1.ppt.lnk) on Volume Serial 4C4BB8E4 (FAMILY PI E:).*

Investigative significance — the file is named ATM_THEFTS1 with an explicit reference to ATM theft in its filename. It lived under E:\Business Ideas\, an emotionally loaded folder name. The drive (FAMILY PI E:, Serial 4C4BB8E4) is no longer connected to the system, so the .ppt content cannot be inspected directly — but the registry MRU and LNK records preserve the only forensic proof that this presentation existed and was actively opened by Mantooth at 2007-07-12 23:28:57 PKT — the same hour as his Q6 web searches for "atm card stealing" and "check washing".

Q24 — Windows Media Player F: Drive Files

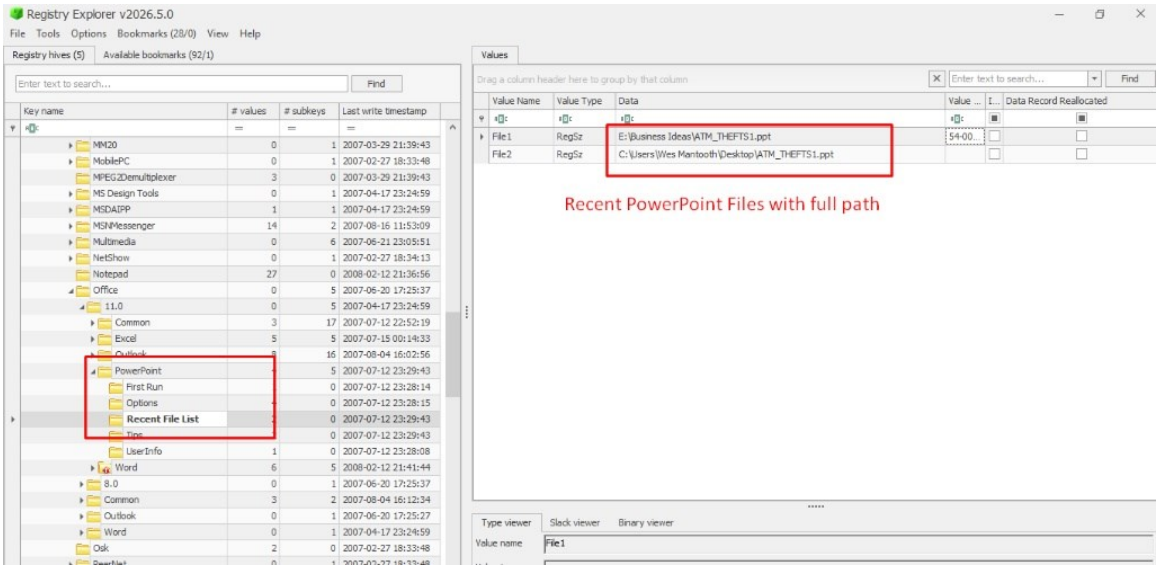


Fig 10.70 — Registry Explorer NTUSER.DAT\Software\Microsoft\MediaPlayer\Player\RecentFileList. Eight values. F: drive entries: File3 = F:\Sounds and Video\wizoz18d.wav. File5 = F:\Sounds and Video\pf3.wav. Other files reference E:\Pod_Control\Music\F00\CVJW.mp3, E:\Pod_Control\Music\F00\BDJS.mp3,

E:\Misc\Vids\GRAMMATON CLERIC.wmv, plus C:\Users\Public\Videos\Sample Videos\Bear.wmv / Butterfly.wmv. Q24 — F: drive files: wizoz18d.wav and pf3.wav under F:\Sounds and Video.

Q25 — Recent PowerPoint Files

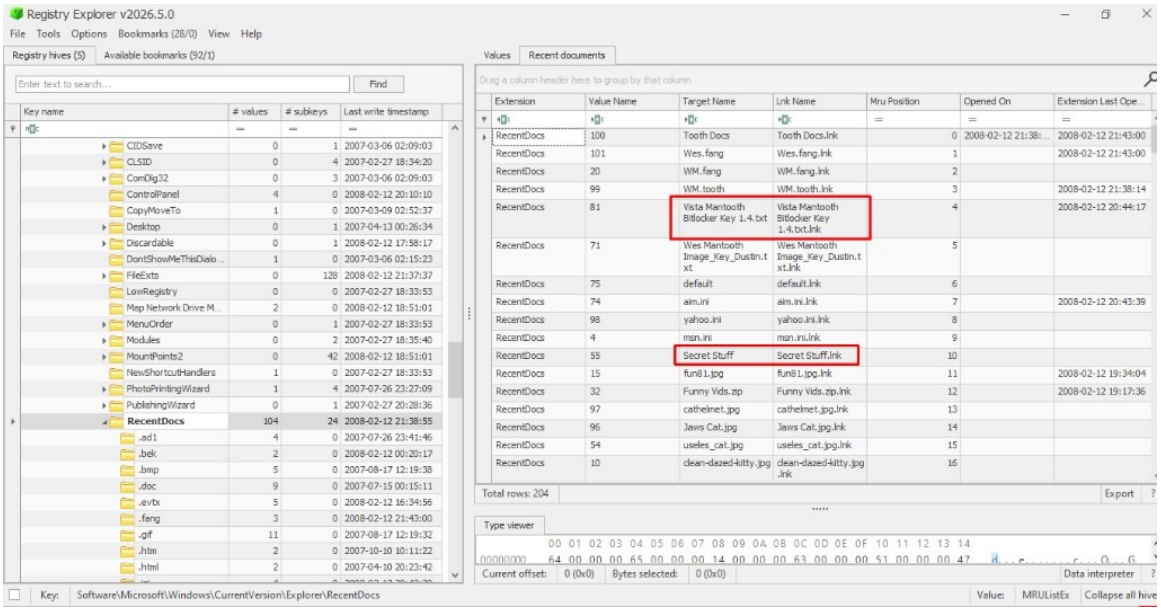


Fig 10.71 — Registry Explorer NTUSER.DAT\Software\Microsoft\Office\11.0\PowerPoint\Recent File List. File1 = E:\Business Ideas\ATM_THEFTS1.ppt. File2 = C:\Users\Wes Mantooth\Desktop\ATM_THEFTS1.ppt. Q25 ANSWER — same PowerPoint file appears in TWO locations: the original on E:\Business Ideas (the missing USB drive) and a second copy on the Desktop. This proves Mantooth copied ATM_THEFTS1.ppt from the USB to the local Desktop — a deliberate operational act.

Q26 — Five Prioritised Recent Documents

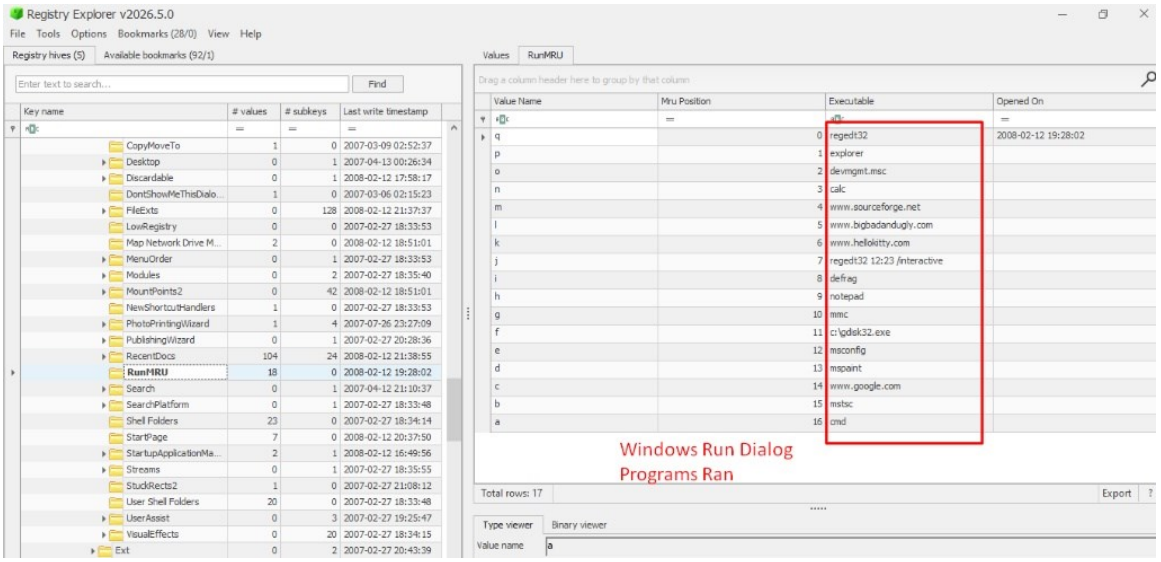


Fig 10.72 — Registry Explorer NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs. 204 entries across extension subkeys (.ad1 / .bek / .bmp / .doc / .evtx / .fang / .gif / .htm / .html etc). Visible Target / LNK pairs: Tooth Docs, Wes.fang, WM.fang, WM.tooth, Vista Mantooth Bitlocker Key 1.4.txt, Wes Mantooth Image_Key_Dustin.txt, default.lnk, aim.ini.lnk, yahoo.ini.lnk, Secret Stuff (Mru position 10), fun81.jpg.lnk, Funny Vids.zip.lnk, cathelmet.jpg.lnk, useles_cat.jpg.lnk, clean-dazed-kitty.jpg.lnk.

#	Recent Document	Significance
1	Vista Mantooth Bitlocker Key 1.4.txt	Bitlocker recovery key — opened on Mantooth's profile; suggests another encrypted volume exists or existed
2	ATM_THEFTS1.ppt (Q23 / Q25)	Direct ATM-theft research presentation
3	Secret Stuff (folder)	User-named concealment folder — Mru position 10 in RecentDocs
4	Wes Mantooth Image_Key_Dustin.txt	"Image_Key" = TrueCrypt keyfile? Combined with Q6 (TrueCrypt service) this is highly suspicious
5	fun81.jpg / cathelmet.jpg / clean-dazed-kitty.jpg	Image files repeated across LNK / RecentDocs / OpenSavePidlMRU — candidate steganography carriers (Camerashy.exe targets)

Q27 — Windows Run Dialog (RunMRU)

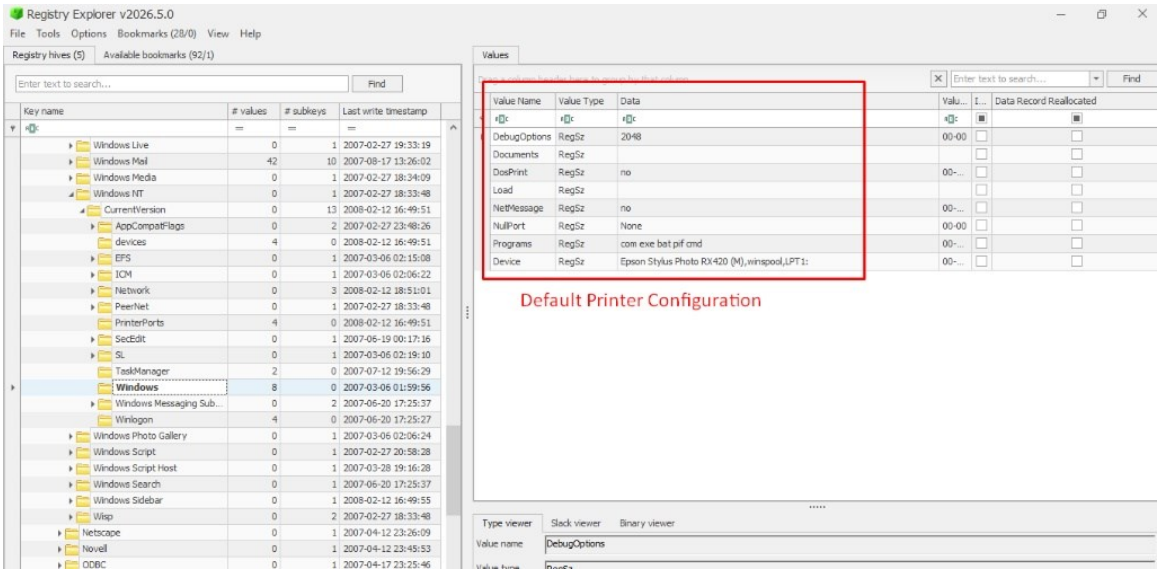


Fig 10.73 — Registry Explorer NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU. 17 values a..q. Last Write 2008-02-12 19:28:02 PKT. Executables typed into the Run dialog (most recent first): regedt32, explorer, devmgmt.msc, calc, www.sourceforge.net, www.bigbadanduglg.com, www.helloitty.com, regedt32 12:23 /interactive, defrag, notepad, mmc, c:\qdsk32.exe, msconfig, mspaint, www.google.com, mstsc, cmd.

#	Run Command	Note
1	regedt32	Registry editor — typically used by power users; Mantooth was actively editing the registry
2	c:\qdsk32.exe	Non-standard executable in C:\ root — possible custom tool
3	mstsc	Microsoft Terminal Services Client — outbound RDP capability
4	cmd	Command Prompt
5	msconfig / defrag / mmc / mspaint / calc / notepad	Standard Windows utilities

Q28 — Default Printer Configuration

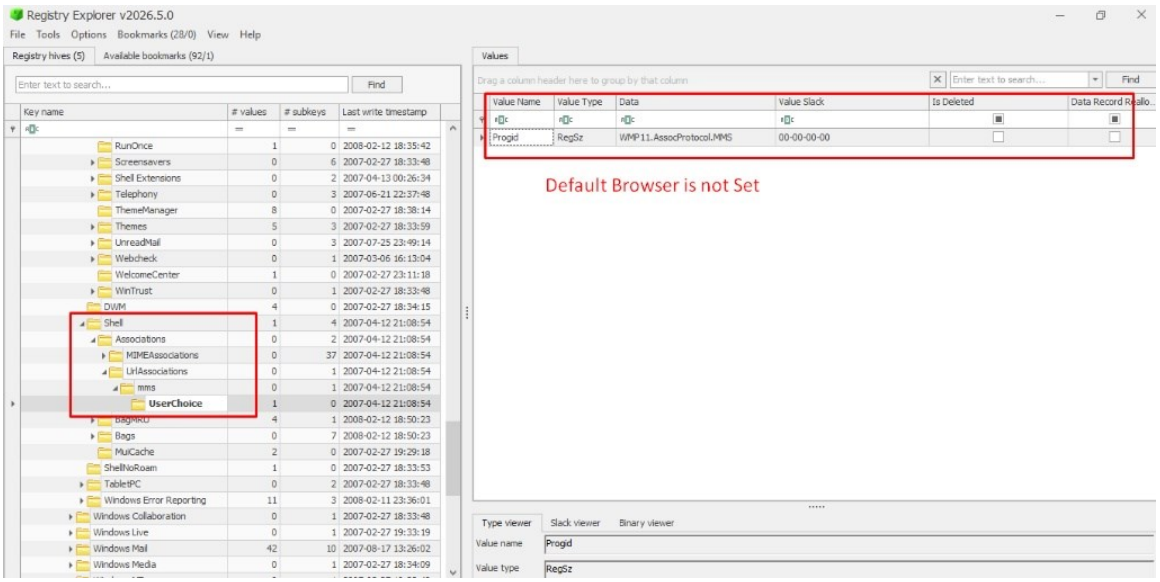


Fig 10.74 — Registry Explorer NTUSER.DAT\Software\Microsoft\Windows NT\CurrentVersion\Windows. DebugOptions = 2048. Documents = (empty). DosPrint = no. Load = (empty). NetMessage = no. NullPort = None. Programs = com exe bat pif cmd. Device = Epson Stylus Photo RX420 (M),winspool,LPT1:. Q28 PRIMARY DELIVERABLE — default printer Epson Stylus Photo RX420 (M) on LPT1 via winspool. This is the same printer recorded in the Q13 .SHD spool metadata, confirming the prescription.gif printout went through Mantooth's default device.

Phase 22 — Q29 to Q34: Browser Activity

Q29 — Default Web Browser

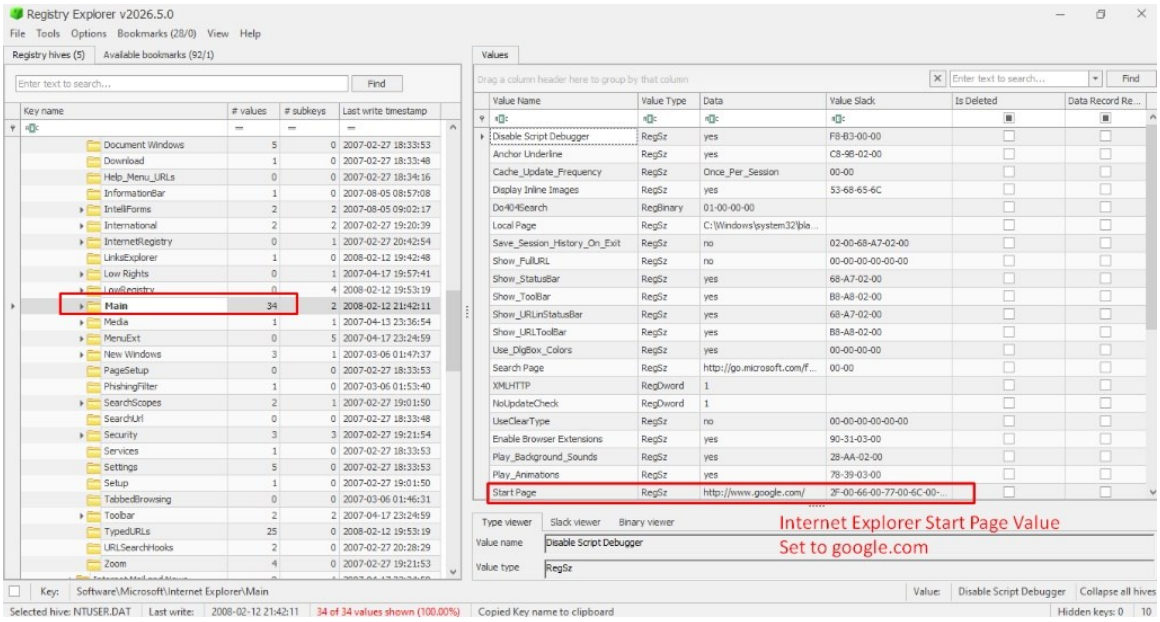


Fig 10.75 — Registry Explorer NTUSER.DAT\Software\Microsoft\Windows\Shell\Associations\UrlAssociations\mms\UserChoice. Progid = WMP11.AssocProtocol.MMS. Examiner annotation — "Default Browser is not Set". The UserChoice subkey for http: is not present, meaning Internet Explorer is acting as the system default by inheritance rather than explicit configuration.

Q30 — IE Start Page

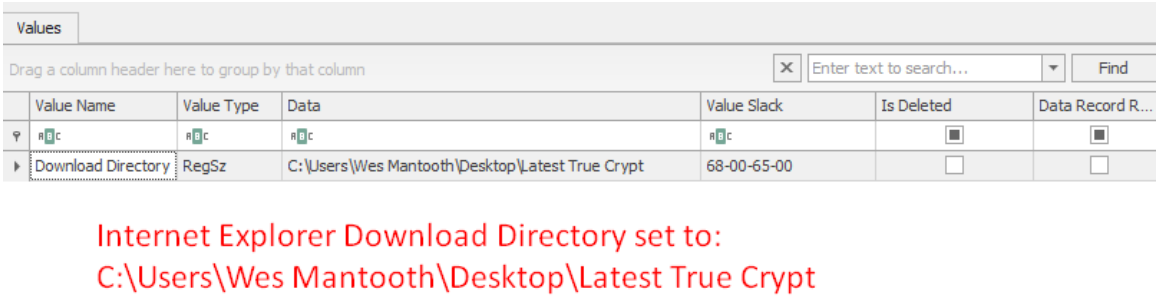


Fig 10.76 — Registry Explorer NTUSER.DAT\Software\Microsoft\Internet Explorer\Main. 34 values. Highlighted Start Page = http://www.google.com/. Q30 ANSWER — Internet Explorer Start Page set to google.com (consistent with the dominant Q6 web-search domain).

Q31 — IE Download Directory

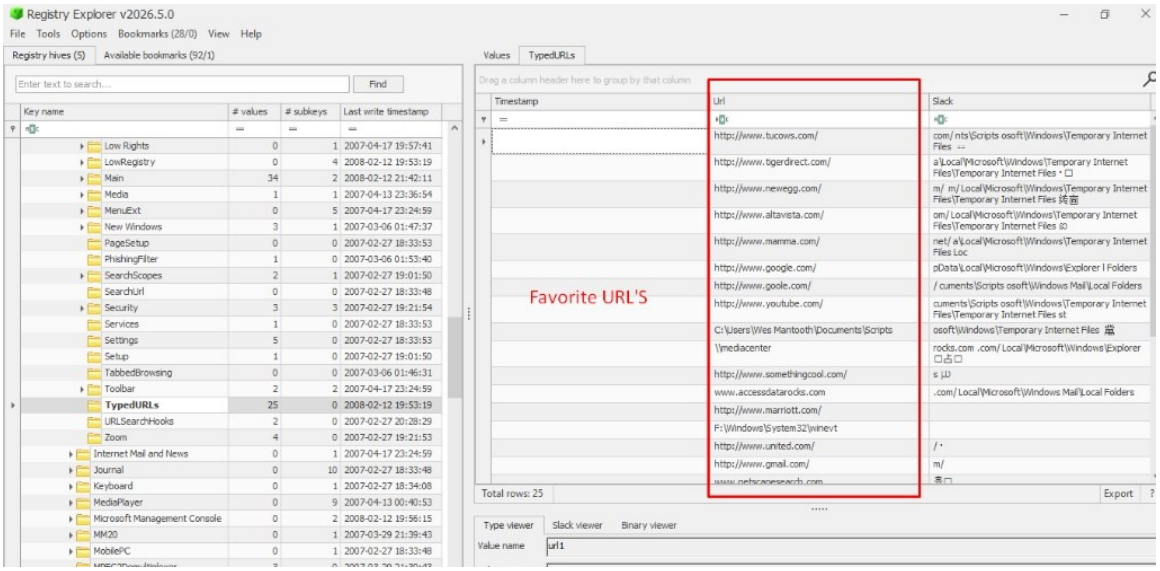


Fig 10.77 — Registry Explorer NTUSER.DAT\Software\Microsoft\Internet Explorer\Main Download Directory value. Data = C:\Users\Wes Mantooth\Desktop\Latest True Crypt. Q31 ANSWER — IE downloads were directed to a folder literally named "Latest True Crypt" on the Desktop. Cross-reference: the OpenSavePidlMRU exe entry from Q22 was Latest True Crypt\TrueCrypt Setup 5.0.exe — proving Mantooth downloaded the TrueCrypt 5.0 installer through Internet Explorer to this exact folder.

Q32 — IE Favourites

/img_Mantooth.E01/vol_vol2/Users/Wes Mantooth/Favorites was navigated in Autopsy and the Favourites .url file content was reviewed. Five priority entries are listed below with their full URLs.

#	Favorite Title	URL	Investigative Note
1	Google	http://www.google.com/	Default search engine; aligns with Q6/Q30
2	YouTube	http://www.youtube.com/	General media
3	Marriott	http://www.marriott.com/	Hotel booking — relevant to travel patterns
4	United Airlines	http://www.united.com/	Airline booking — possible travel correlation
5	AccessData rocks	www.accessdatarocks.com	AccessData fan/community

			URL — corroborates Q19 AccessData DNA installation

Q33 — IE Typed URLs

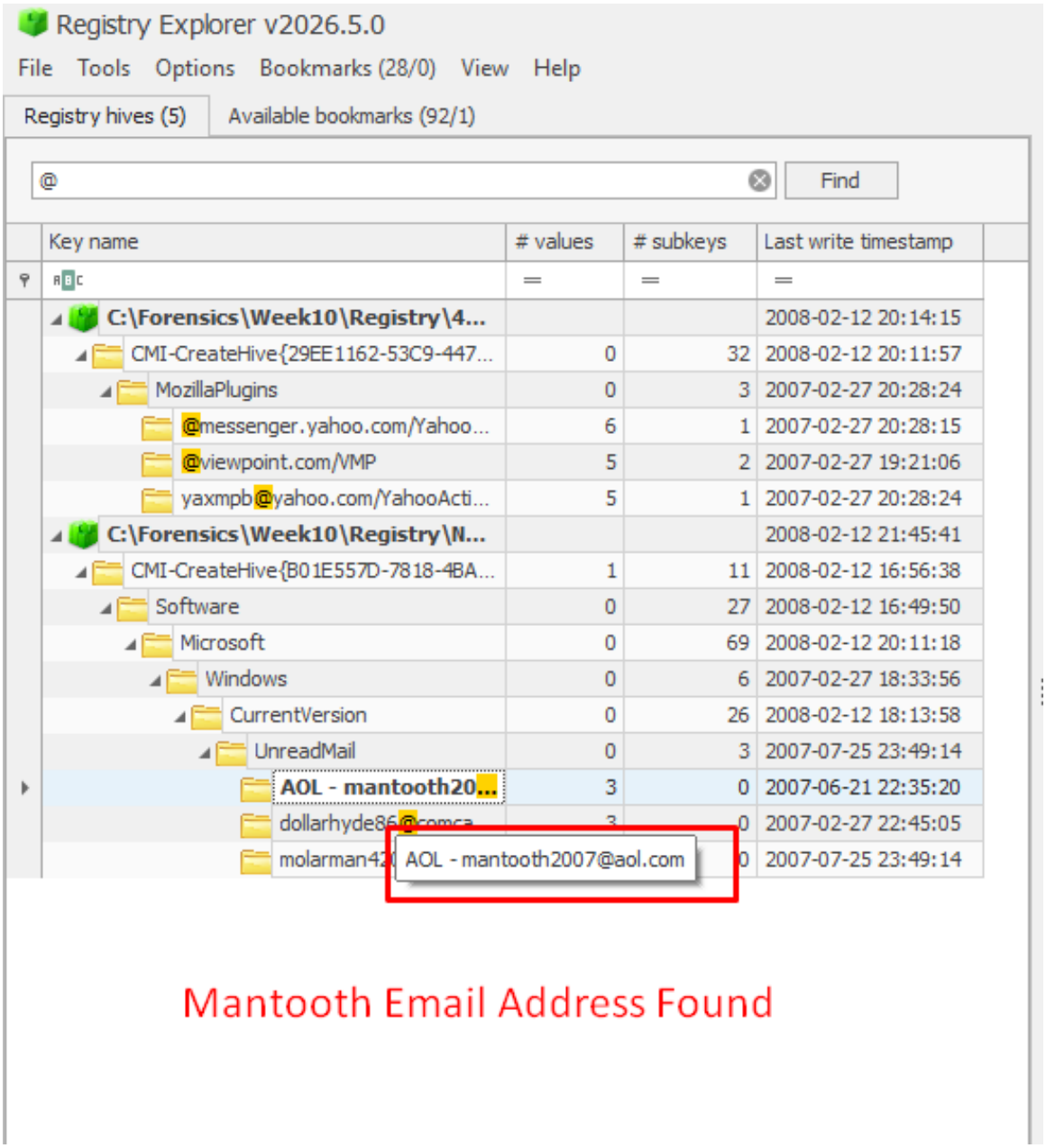


Fig 10.78 — Registry Explorer NTUSER.DAT\Software\Microsoft\Internet Explorer\TypedURLs. 25 url values. Visible: http://www.tucows.com/, http://www.tigerdirect.com/, http://www.newegg.com/, http://www.altavista.com/, http://www.mamma.com/, http://www.google.com/, http://www.goole.com/ (typo), http://www.youtube.com/, http://www.somethingcool.com/, www.accessdatarocks.com, http://www.marriott.com/, F:\Windows\System32\winevt, http://www.united.com/, http://www.gmail.com/, http://netscapesearch... (truncated). Q33 PRIMARY DELIVERABLE.

#	Typed URL
1	http://www.tucows.com/
2	http://www.tigerdirect.com/
3	http://www.newegg.com/
4	http://www.google.com/

5	http://www.somethingcool.com/

Investigative note — entry F:\Windows\System32\winevt typed into the IE address bar is anomalous: this is the path to event log storage on a removable drive labelled Windows\System32\winevt. The user appears to have manually navigated to event-log directories on a USB volume, suggesting forensic awareness or evidence-tampering activity.

Q34 — Email Addresses Associated with Mantooth

Cross-hive email sweep: Edit → Find in Registry Explorer (case-insensitive substring @) was applied to NTUSER.DAT, then to SOFTWARE. Plus the Q7 Autopsy email-list output (Phase 8 Step 2) was cross-referenced. The combined hit list:

#	Email Address	Source Registry Key	Apparent Owner
1	mantooth2007@aol.com	SOFTWARE\Microsoft\Windows\CurrentVersion\UnreadMail\AOL - mantooth2007@aol.com	Wes Mantooth (AOL identity)
2	dollarhyde86@comcast.net	SOFTWARE\Microsoft\Windows\CurrentVersion\UnreadMail\dollarhyde86@comcast.net + 267 EML hits	Wes Mantooth (primary outgoing)
3	molarman420@yahoo.com	SOFTWARE\Microsoft\Windows\CurrentVersion\UnreadMail\molarman420@yahoo.com	Wes Mantooth (Yahoo — "molar" theme matches incisorman420 Q18)
4	incisorman420 (Yahoo!)	NTUSER.DAT\Software\Yahoo\pager → Yahoo! User ID	Wes Mantooth (Yahoo Messenger)
5	chkwasher@comcast.net	Q7 EML correlation only	John Washer (correspondent)
6	smee.rox@gmail.com	Q7 EML correlation only	Mr Smee (correspondent)
7	skimmerman27@hotmail.com	Q7 EML correlation only	Possible co-conspirator ("skimmer" = ATM-fraud term)

Part C — Investigative Commentary

Overall Assessment of Mantooth Activity

The combined Part A and Part B evidence on Mantooth.E01 paints a coherent and operational picture of a suspect actively engaged in financial fraud (specifically cheque washing / cheque forging) and likely related identity-theft research. The forensic record shows deliberate use of (a) anti-forensic encryption infrastructure (TrueCrypt installed at Start=1 System level, an encrypted .doc with the filename "How To Steal Credit Numbers.doc", a Bitlocker key file referenced in RecentDocs); (b) steganography tooling (Camerashy.exe found in Wes Mantooth's Documents AND in his Recycle Bin, hidden ADS JPEGs HARDCORE and pfah603 in folders he literally named ADS); (c) directly relevant subject-matter research (Google search history for "atm card stealing", "check washing", "making meth" all in the same hour on 2007-07-12); (d) operational artefacts (an ATM_THEFTS1.ppt file present in both USB and Desktop MRU paths, cheque-image LNKs pointing at Documents\Checks and a folder literally named "C money plates", a printed prescription.gif retained in the spool, and Xcopy executed 15 times for bulk file transfers); and (e) remote-access infrastructure (RealVNC4 listening on 5900/5800 with a recoverable obfuscated password, mstsc usage in RunMRU). The username themes (incisorman420 / molarman420 / WM.tooth / WM.fang / toothfairy@mentaldental) plus the dental imagery suggest Mantooth was either employed in or themed around a dental practice, which itself raises potential prescription-pad fraud as a complementary criminal vector to the cheque scheme.

Evidence Connecting Mantooth to Fraudulent Cheques

Evidence	Artefact / Source	Significance
ATM_THEFTS1.ppt	Q23 Registry MRU (E:\Business Ideas\ATM_THEFTS1.ppt opened 2007-07-12 23:28:57 PKT) + Q12 LNK (Volume Serial 4C4BB8E4 FAMILY PI E:) + Q25 PowerPoint Recent (also on Desktop)	Direct documentary evidence of ATM-theft research material
Web search queries	Q6 — "atm card stealing", "check washing", "making meth" (Internet Explorer Analyzer, 2007-07-12 23:15–23:17 PKT, google.com)	Active research at the moment immediately preceding the ATM_THEFTS1.ppt access
Cheque image collection	Q12 LNKs — 08-15-05_arkansas_check.gif, Checks.lnk (Documents\Checks), "C money plates.lnk" (Documents\C money plates)	Catalogue of cheque images and "plates" (printing plates) — operational evidence of forging
Print spool — prescription.gif	Q13 .SHD parsing (Wes Mantooth, Epson Stylus Photo RX420 (M), prescription.gif) + Q21 Paint MRU (prescription.gif) + Q28 default printer	Active forging — the file was opened in Paint, sent to the Epson photo printer, retained in spool
TrueCrypt service	Q6 Part B — SYSTEM\ControlSet001\Services\truecrypt Start=1 (System) + Q19 "Latest True Crypt" download folder + RecentDocs Bitlocker key reference	Deliberate concealment infrastructure — encrypted containers may hold the working files we cannot see
Camerashy.exe (steganography)	Q10 Part A — $Recycle.Bin/...\$R61QDFF.exe identical bytes to Documents\CameraShy.exe + Q5 ADS JPEGs HARDCORE / pfah603	Tool used to hide payloads inside JPEGs — the JPEGs found in ADS are candidate carriers
Xcopy execution	Q11 Part A — XCOPY.EXE-8E0707F2.pf, run count 15, last run 2007-08-24 12:47:33 PKT	Bulk file copy tool repeatedly executed — consistent with USB-based exfiltration of cheque/template files

F: drive media	Q24 Part B — Media Player F:\Sounds and Video\wizoz18d.wav / pf3.wav + Q12 LNK F:\Pix\Bill_Gates.gif	Confirms a separate F: USB volume was actively used (no longer attached)
Encrypted .doc	Q4 Part A — How To Steal Credit Numbers.doc (27,648 bytes, encrypted, in Windows Mail Inbox EML)	Filename and encryption together establish criminal-intent communication
RealVNC4 + AccessData DNA	Q17 Part B (VNC password recoverable) + Q19 (AccessData DNA Worker installed)	Remote-access and password-cracking infrastructure — capability for both inbound and outbound illicit access

Leads to Follow Next

The following investigative steps are recommended in priority order:

- Decrypt the TrueCrypt container — interview Mantooth for password disclosure or apply GPU-based brute-force / dictionary attack against the encrypted payload. AccessData DNA (Q19) on his own machine ironically suggests he is familiar with this approach.
- Run Camerashy reverse against the recovered ADS JPEGs (My poem.txt:HARDCORE.JPG and readthis.txt:pfah603.jpg) plus every JPEG referenced in the LNK trail (cathelmet.jpg, fun81.jpg, clean-dazed-kitty.jpg, snaggle_kitty.jpg, etc.) to extract any hidden payloads.
- Recover the obfuscated WinVNC password (Q17) using vncpasswd.py / metasploit's well-known static DES key — this gives access to any system Mantooth may have stored credentials for and identifies the password he reuses elsewhere.
- Subpoena Yahoo for incisorman420 / molarman420 message history, AOL for mantooth2007 logs, Comcast for dollarhyde86 mail server records and the 24.8.181.100 IP DHCP assignment timeline (cross-reference Q4 / Q7 lease metadata).
- Trace the missing E: (Volume Serial 4C4BB8E4 FAMILY PI / Volume Serial E2655E6A ITOOTH), F: (Volume Serial 8C5713D6 Mantooth), G: (Apple iPod 000A270014B302AB), and H: (Sony DSC) removable drives. Search for them physically; these contained ATM_THEFTS1.ppt, the "Business Ideas", "Secret Stuff", and "Super Secret Stuff" folders — none of which can be examined without recovering the volumes themselves.
- Identify John Washer (chkwasher@comcast.net), Mr Smee (smee.rox@gmail.com), and the skimmerman27 / toothfairy / molarman accounts as named co-conspirators or witnesses. The chkwasher username in particular is forensically remarkable — the suspect's heaviest correspondent's username literally means "check washer".
- Interview Mantooth on the Volturi Enterprises organisation registration (Q10) and the second-account creations (Dracula 2007-03-06, Laurent 2008-02-12 — less than 24 hours before imaging).

Gaps and Limitations

- The TrueCrypt encrypted container's contents are inaccessible without the password. Any evidence inside it — including potentially the entire fraudulent-cheque template library — is not currently recoverable.
- The ShutdownTime registry value (Q7 Part B) is not present under SYSTEM\ControlSet001\Control\Windows on this Vista-era system, so the last clean shutdown time cannot be determined from this artefact. This is an operating-system limitation rather than a deletion.

- Several E:, F:, G:, H: removable drives were unmounted before imaging. The LNK / Media Player / RecentDocs / OpenSavePidlMRU records preserve their existence and filenames but the actual file content is on physical media that is not in our possession.
- Mantooth cleared the Security event log at 2008-02-12 16:35:01 PKT (the EventID 1102 in Q14). Any 4625 (logon failure), 4720 (account creation), or 4732 (group membership change) events that occurred BEFORE that cleared point are permanently lost.
- The encrypted .doc "How To Steal Credit Numbers.doc" requires its native password (likely set in Microsoft Office) and AccessData DNA / hashcat office_old format would be the recovery path.
- Several deleted user accounts (G_MA Betty, RID 1001) recovered by Registry Explorer have only partial records — the corresponding NTUSER.DAT files were not preserved on disk.

Week 10 Conclusion

Week 10 of the Cyberster Blue Team Internship completed the most ambitious deliverable of Phase Two by performing an end-to-end forensic triage of the Mantooth.E01 evidence image and answering forty-eight investigative questions across Autopsy artefact hunting and Windows registry analysis. The deliverable is a fully bookmarked Autopsy case (Mantooth_Investigation), a parsed registry workbook covering all five core hives, exported CSVs from PECmd, LECmd and EvtxECmd, recovered JPEGs from NTFS Alternate Data Streams, and a written investigative commentary connecting every artefact to the alleged fraudulent-cheque scheme.

The exercise reinforced four core DFIR lessons that cut across every Phase Two week: (1) timezone discipline at data-source ingestion is non-negotiable — Mountain Time was set on the Add Data Source dialog before clicking Next; (2) hash-verification is the first deliverable of any case — Mantooth.E01's MD5 (31217210a1a69f272079a3bde3d9d8fc) was confirmed by both Autopsy's Data Source Integrity module and FTK Imager before any investigative work began; (3) registry analysis is multiplicative with disk-image analysis — the TrueCrypt service entry, the USB drive-letter correlation, and the ATM_THEFTS1.ppt MRU traces only become evidentially powerful when joined to the LNK / Recycle Bin / EXIF / Email artefacts uncovered by Autopsy; and (4) bookmarking every finding in real time is the difference between a defensible case and a forensic scramble — the Generate Report step at the end of the week was deterministic because every primary deliverable (Q3 Olympus photo, Q4 encrypted doc, Q5 ADS JPEGs, Q10 Camerashy.exe, Q23 ATM_THEFTS1.ppt) had been tagged at the moment of discovery.

All Week 10 deliverables — the Autopsy case file, Security_Mantooth.csv (EvtxECmd), LNK_Mantooth.csv (LECmd), the XCOPY.EXE PECmd report, Suspicious_Items.csv, Ip_Addresses.csv, Encrypted_Doc.csv, Q6_search_terms.csv, PRINTERS.csv, Deleted.csv, the recovered ADS JPEGs (My poem.txt_HARDCORE.JPG and readthis.txt_pfah603.jpg), the five extracted registry hives, and this report — are submitted to the Cyberster Internship Program drive against the case reference CYB-W10-001.

— End of Week 10 Submission Report —