Cyberster

INTERNSHIP REPORT

A Weekly Progress and Learning Summary

Phase Two : Email Forensics and Super Timeline Analysis

Submitted to: Cyberster Internship Program

Intern Name: Abdul Muqeet Tabraiz

Roll Number: CSI-B1-353

Email Header Analysis | PST & MBOX Parsing | plaso (timeline) | RegistryExplorer | eECmd | Integrated Timeline View | Forensic Artifact Hunting

A Weekly Progress and Learning Summary

Table of Contents

Annex D - PECmd Files Referenced (Complete List)

Annex E - Filtered Timeline CSV (jean_filtered_timeline_0125_0130.csv)

Week 11 Overview

Week 11 of the Cyberster Blue Team Internship is a deliberate shift in investigative posture. Where Week 10 was a wide, cataloguing triage across more than a dozen artefact categories of the Mantooth.E01 image, Week 11 is the opposite: a narrow, anchored, three-part investigation of a single known file (m57plan.xls / m57biz.xls), a single known timestamp (2008-07-20 01:28:03 UTC, from the task brief), and a single central question - is Jean, the CFO of M57.biz, more consistent with an insider who intentionally exfiltrated a confidential spreadsheet, or with a user who responded in good faith to a deceptive request?

Part A (Days 74-75) is Email Extraction and Initial Triage. Jean's split EnCase image (nps-2008-jean.E01 + nps-2008-jean.E02) is ingested into Autopsy 4.22.1 with the data source timezone explicitly set to GMT/UTC. The Email Parser module surfaces Jean's outlook.pst archive at Local Settings\Application Data\Microsoft\Outlook\outlook.pst. The Default folder under Results -> E-Mail Messages reports 261 parsed messages. Within those 261, the operationally relevant outbound reply RE: Please send me the information now (sent 2008-07-20 01:28:00 UTC by Jean User <jean@m57.biz>, attaching m57biz.xls, 291,840 bytes) is identified. The raw message body, accessed via the Text tab in Autopsy's lower pane, contains the quoted Original Message block of the inbound request Jean was replying to. That quoted block reads From: alison@m57.biz [mailto:tuckgorge@gmail.com] - i.e. the display portion shows alison@m57.biz but the underlying mailto address embedded in the message is tuckgorge@gmail.com. This discrepancy is the forensic pivot of the case.

Part B (Days 76-78) is the Host-Based Artefact Deep-Dive. Three independent on-disk artefact categories are extracted from the image and parsed with Eric Zimmerman's command-line tools. m57biz.lnk from Jean\Recent is parsed with LECmd 2026.5.0; the LECmd output reports Target Created / Modified / Accessed all equal to 2008-07-20 01:28:03 UTC, Machine ID jean-13fbf038a3, MAC 00:0c:29:8d:35:2b (VMware OUI), Volume Serial 744FC21F. EXCEL.EXE-1C75F8D6.pf from Windows\Prefetch is parsed with PECmd 2026.5.0; the PECmd output reports Last Run 2008-07-20 01:27:40 UTC, Run Count 2, and a 59-entry Files Referenced list that explicitly contains M57BIZ.XLS at row 38 of the list (Keyword: True). NTUSER.DAT is loaded into Registry Explorer 2026.5.0; the RecentDocs\.xls subkey has last write 2008-07-20 01:28:04 UTC with Target Name m57biz.xls and Lnk Name m57biz.lnk, and the Office\11.0\Excel\Recent Files subkey has last write 2008-07-20 01:28:13 UTC with File1 = C:\Documents and Settings\Jean\Desktop\m57biz.xls. All three artefact categories cluster within 33 seconds of each other and are internally consistent.

Part C (Days 79-80) is the Super Timeline. Autopsy's built-in Timeline module is generated against the already-ingested data source (Plaso event ingestion ran during the original Add Data Source pass), then progressively filtered using the Start Big - Filter Down methodology from the task brief. Stage-by-stage event counts: unfiltered = 1,000,000+ (Plaso-indexed events across the full image, 1970 epoch to 2008); date filter 2008-07-20 = 2,017 events; time-window filter 01:23:45 - 01:31:15 UTC = approximately 95 events (visible cluster in the Details view); keyword filter m57biz = 8 unique events (the deliverable CSV).

The eight events reorder by timestamp into a single-second narrative: Excel prefetch run at 01:27:40, Office MRU and Explorer Recent Documents writes at 01:27:42, Outlook outbound + self-Received envelope at 01:28:00, file system Modified / Changed events on the Desktop spreadsheet and on the outlook.pst attachment store at 01:28:03 - 01:28:04.

Part D synthesises the three preceding parts into a single investigative narrative. The host artefact chain confirms Jean physically operated the workstation, opened m57biz.xls in Excel, and composed a reply with the spreadsheet attached. The email evidence shows the reply was directed to an underlying address (tuckgorge@gmail.com) different from the alison@m57.biz display the user would have seen. The evidence is therefore more consistent with Jean responding in good faith to a deceptive request than with deliberate malicious exfiltration; the deceptive request originates from the operator of tuckgorge@gmail.com.

Methodology, Identities, and Chain of Custody

Timezone Handling

Every timestamp in this report is presented in Coordinated Universal Time (UTC, equivalent to GMT for this case period; the case window does not cross any leap-second boundary). The Add Data Source wizard timezone was explicitly set to (GMT+0:00) UTC before clicking Next, so all Autopsy artefact timelines and the Timeline Editor (in its GMT/UTC display mode) report in UTC. Eric Zimmerman's LECmd and PECmd tools both parse timestamps directly from on-disk binary structures and emit UTC by design. Registry Explorer renders last-write timestamps in UTC when loaded against an offline hive.

Some Autopsy file-browser table columns (Modified Time, Change Time, Access Time, Created Time) render the underlying NTFS MFT $STANDARD_INFORMATION timestamps in the examiner workstation's local timezone rather than UTC, even when the data source timezone is set to UTC. This is Autopsy's documented behaviour for the file-listing pane (as distinct from the Timeline pane). Where this report quotes a screenshot caption that shows local-timezone values, the corresponding UTC value used in the corroboration tables, sequence reconstruction, and conclusion is taken directly from the tool-level UTC outputs (LECmd, PECmd, Registry Explorer, Timeline Editor in GMT/UTC mode), and is not derived by manual offset arithmetic against the file-browser display. This avoids any risk of daylight-saving or timezone-database edge cases corrupting the analysis.

Identities

The case involves multiple email identities and three are easily confused. They are defined once here and used consistently throughout the report.

Identity (as written)	What it refers to
Jean / Jean User <jean@m57.biz>	The subject of the investigation - CFO of M57.biz, owner of the disk image nps-2008-jean.E01, and the user whose Outlook 2000 archive (outlook.pst) was parsed.
Allison	Used in this report and in the task brief as the everyday English spelling for the President of M57.biz, the apparent intended recipient of the m57biz.xls spreadsheet.
Alison / alison@m57.biz	The exact lowercase-display spelling that appears as the display name on the inbound lure message (Result 224 of 305) and on Jean's outbound reply (Result 261 of 305). When this report writes alison@m57.biz it refers to the display string in the email headers, not to the human identity Allison.
alex <alison@m57.biz>	A separate, benign, continuously-used display identity that appears as the From: line on Allison's normal day-to-day correspondence with Jean (Google Alerts forwarding, CNN.com Top 10, programmers, background checks, which email address are you using?, etc.). The lower-case alex prefix is the distinguishing fingerprint of this benign identity. It is genuinely Allison's working identity for personal/internal email and is not under suspicion in this case.

tuckgorge@gmail.com	The underlying mailto address embedded in the inbound lure message (Result 224 of 305) and visible as the From: line on the Thanks! follow-up acknowledgement (Result 223 of 305). This is a personal Gmail address operated by a third party who is impersonating the alison@m57.biz display identity.

Chain of Custody

- The instructor-supplied evidence E:\Cyberster Internship\Week 11\Jean Disk Image\nps-2008-jean.E01 and the matching segment file nps-2008-jean.E02 were preserved on a separate volume from the examiner working folder C:\Forensics\Week11\, and were never written to during the examination.
- The image was read by Autopsy in read-only mode (the default for Disk Image or VM File data sources). Every artefact discussed in this report - LNK, prefetch, NTUSER.DAT hive, individual emails - was extracted into the examiner working folder as a derived copy via Autopsy's Extract File(s) right-click action. The original bytes inside the E01/E02 pair were not modified by the examination.
- Autopsy's Data Source Integrity (Hash Lookup) module computed MD5 of nps-2008-jean.E01 = 78a52b5bac78f4e711607707ac0e3f93 and compared it against the stored hash embedded in the EnCase E01 metadata. Result: verified. The image is bit-for-bit identical to the instructor-supplied original.
- All derived artefacts (m57biz.lnk, EXCEL.EXE-1C75F8D6.pf, NTUSER.DAT, NTUSER.DAT.LOG, LECmd CSV outputs, PECmd CSV outputs, jean_filtered_timeline_0125_0130.csv) are listed in Annex A with their on-disk paths in the examiner working folder and a one-line description of their derivation source.
- Where this report quotes from a parsed email body (Annex B), the quoted text is taken from Autopsy's Text-tab view of the relevant E-Mail Messages row; no edits, redactions, or paraphrases have been applied to the quoted text beyond replacing the verbatim curly apostrophe character with a straight ASCII apostrophe for compatibility with this document's font.

Evidence vs Interpretation Notation

Where individual findings warrant structured reporting, this document uses the following labelled blocks: Evidence (the directly observed artefact value or screenshot content); Interpretation (the analyst's reasoned reading of the evidence); Limitation (what the evidence does or does not prove on its own). This notation appears throughout Parts A, B, and C and is intended to keep analyst inference clearly separated from observed data.

Investigation Parameters and Threat Intelligence

The task brief supplies four anchor parameters that every artefact in this report is evaluated against. Anchoring to a known file, a known hash, a known timestamp, and a known time window is the discipline that converts an overwhelming dataset into a defensible narrative - the Start Big, Filter Down methodology referenced in the Week 11 task brief.

Parameter	Value
Target file (task-brief name)	m57plan.xls
Target file (on-disk name)	m57biz.xls (the task brief uses m57plan.xls; the file as it sits on Jean's Desktop in the image is m57biz.xls - both names refer to the same file)
Target file location	C:\Documents and Settings\Jean\Desktop\m57biz.xls
File size	291,840 bytes
File MD5 (instructor-supplied)	e23a4eb7f2562f53e88c9dca8b26a153
Last modified time (anchor)	2008-07-20 01:28:03 UTC
Investigation window (task brief)	2008-07-20 01:25:00 UTC to 01:30:00 UTC
Investigation window (used here)	2008-07-20 01:23:45 UTC to 01:31:15 UTC (a 7.5-minute envelope wrapping the prescribed 5-minute window with extra padding so the Details-view bars render legibly)
Case timezone	(GMT+0:00) UTC, set on the Add Data Source wizard before clicking Next
Image filename	nps-2008-jean.E01 (split with nps-2008-jean.E02, both kept in the same folder)
Image MD5 (verified)	78a52b5bac78f4e711607707ac0e3f93
Suspect	Jean User <jean@m57.biz>, CFO of M57.biz
Apparent recipient (per Jean)	Allison, President of M57.biz (display string alison@m57.biz)
Underlying recipient address (forensic finding)	tuckgorge@gmail.com (mailto address embedded in the inbound lure that Jean replied to)

The case is the FBI-published M57.biz / Jean scenario from Digital Corpora. The disk image is shipped in EnCase split format. Autopsy auto-detects the E02 segment when the E01 is selected; no manual concatenation is needed. The image contains a single Windows XP installation for user Jean with Microsoft Office 2003 (Office\11.0 in the registry) and Microsoft Outlook 2000 as the mail client.

Part A - Email Extraction and Initial Triage (Days 74-75)

Objective

The objective of Part A is to locate, extract, and analyse Jean's email archive from the disk image, isolate the outbound email that carried m57biz.xls as an attachment, and - most importantly - inspect the raw RFC 2822 message body of that email to determine the underlying reply address as distinct from the parsed display name. The task brief is explicit that the display-name-versus-underlying-address discrepancy is the forensic pivot of the entire investigation; if the raw message body is not inspected, the wrong conclusion is reached.

Tools Used

Tool	Source	Used In
Autopsy 4.22.1	sleuthkit.org/autopsy	Days 74-80 (all three parts)
Eric Zimmerman LECmd 2026.5.0	ericzimmerman.github.io	Part B - LNK parser
Eric Zimmerman PECmd 2026.5.0	ericzimmerman.github.io	Part B - Prefetch parser
Eric Zimmerman Registry Explorer 2026.5.0	ericzimmerman.github.io	Part B - NTUSER.DAT analysis
Microsoft Excel	Microsoft 365	LNK and Prefetch CSV inspection
Windows command prompt (cmd.exe)	Windows 10/11 host	LECmd / PECmd invocation

Phase 0 - Tooling and Working Folder Layout

Step 1: Working folder structure

A flat working tree was created under C:\Forensics\Week11\ to hold the Autopsy case directory, the extracted artefacts, the parsed CSVs, and the report assets. The image itself was staged on a separate volume (E:\Cyberster Internship\Week 11\Jean Disk Image\) so the original evidence files remained untouched.

```
C:\Forensics\Week11\
  Week11_M57_Jean\            (Autopsy case directory)
  LNK\                        (Extracted m57biz.lnk + LECmd CSV output)
  Prefetch\                   (Extracted EXCEL.EXE-1C75F8D6.pf + PECmd CSV output)
  Registry\                   (Extracted NTUSER.DAT + NTUSER.DAT.LOG)
  Export\                     (jean_filtered_timeline_0125_0130.csv from Timeline Editor)
```

Phase 1 - Autopsy Case Creation (Week11_M57_Jean)

Autopsy 4.22.1 was launched and File -> New Case opened the Case Information wizard. The Case Name was set to Week11_M57_Jean and the Base Directory was set to C:\Forensics\Week11\. The Case Type radio was left at Single-User. Autopsy auto-computed the final case path

C:\Forensics\Week11\Week11_M57_Jean as the directory where the case database, ingest results, and exported artefacts would live.

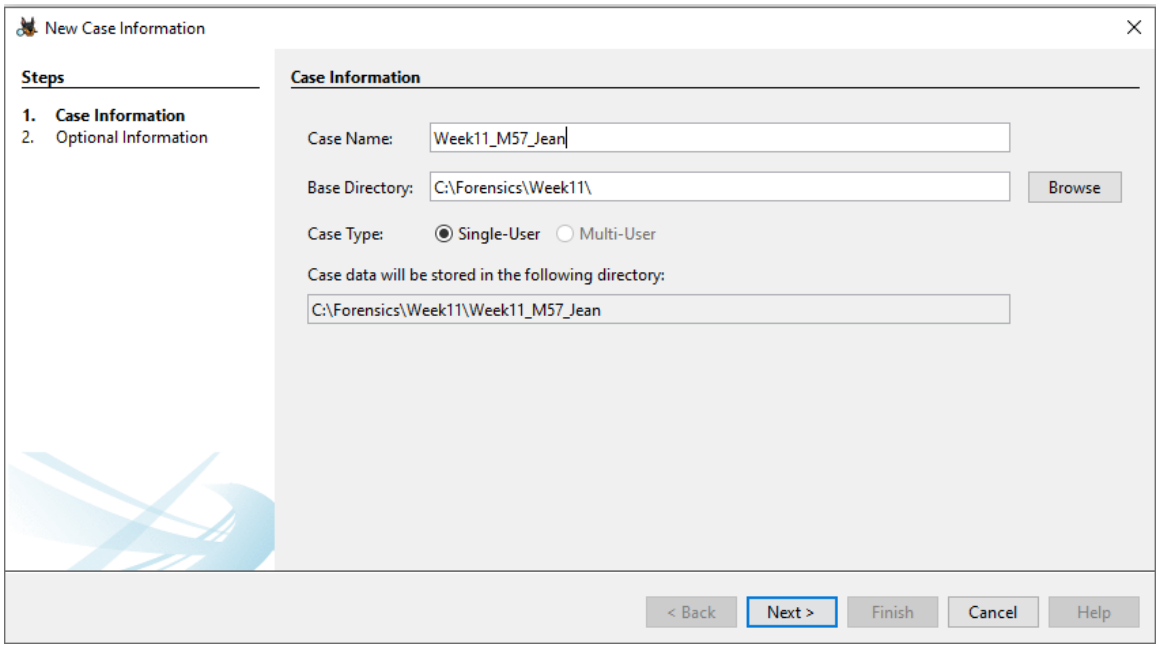


Fig 11.1 - Autopsy New Case Information dialog. Case Name: Week11_M57_Jean, Base Directory: C:\Forensics\Week11\, Case Type: Single-User. Computed case path: C:\Forensics\Week11\Week11_M57_Jean.

Phase 2 - Optional Case Metadata

On clicking Next, the Optional Information page was completed with the case number, examiner identity, and organisational affiliation. The case number W11_001_Jean follows the same convention used in Week 10 (internal week + sequence + suspect). The Phone, Email, and Notes fields were left blank. The Organization dropdown was set to Cyberster Blue Team Internship via the Manage Organizations side panel.

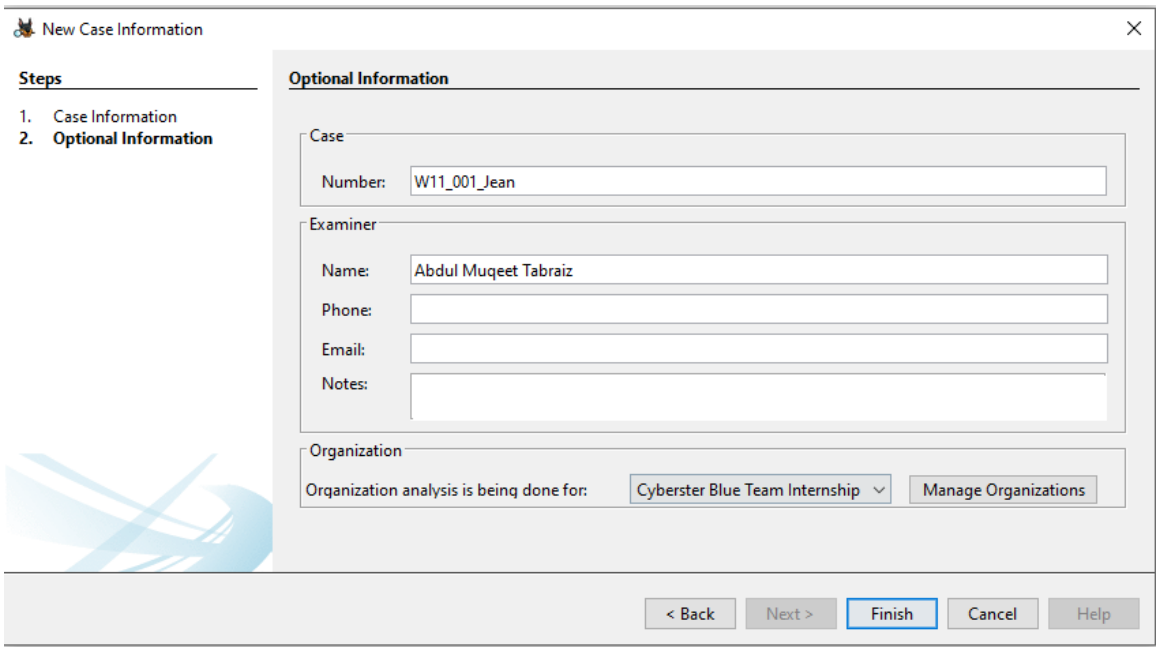


Fig 11.2 - Autopsy Optional Information page. Case Number: W11_001_Jean, Examiner: Abdul Muqeet Tabraiz, Organisation: Cyberster Blue Team Internship.

Phase 3 - Add Data Source and Set Timezone

Step 1: Select Data Source Type

Clicking Finish on the metadata page closed the case creation wizard and launched the Add Data Source wizard. On step 2 of 5 (Select Data Source Type), Disk Image or VM File was selected - the correct option for a split EnCase E01/E02 image.

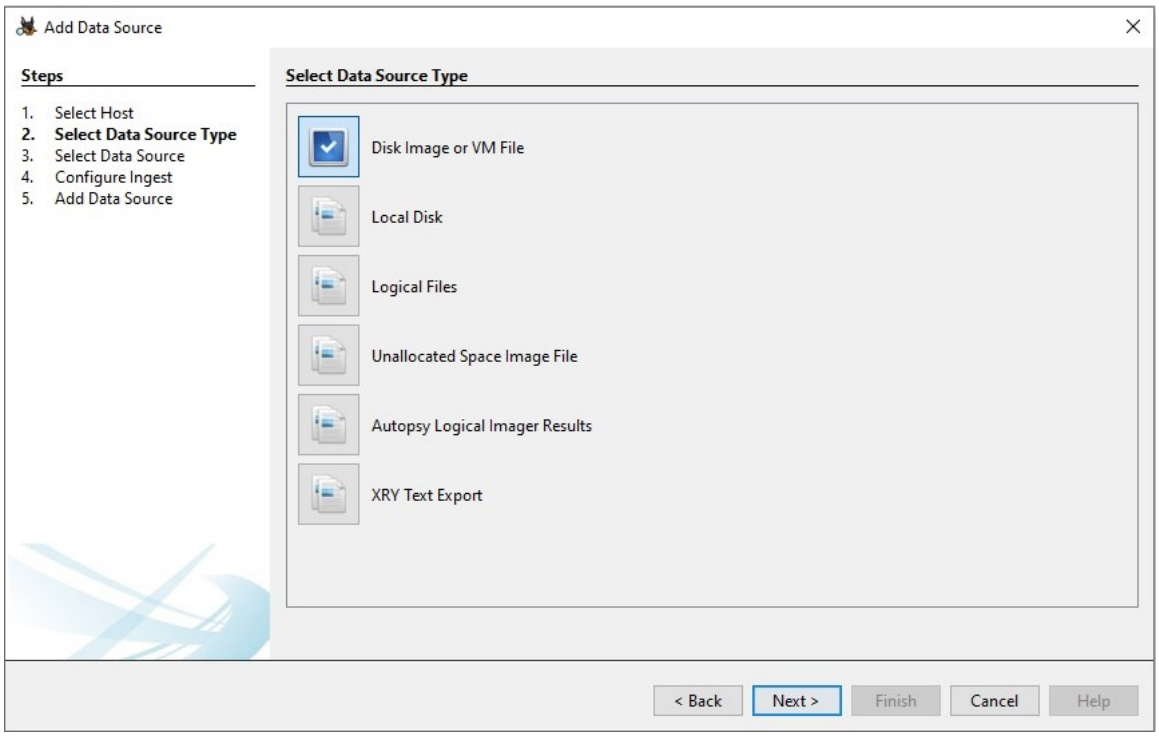


Fig 11.3 - Add Data Source wizard, step 2 of 5. Disk Image or VM File selected as the data source type for nps-2008-jean.E01.

Step 2: Provide the image path AND set timezone

On step 3 of 5 the Path field was browsed to E:\Cyberster Internship\Week 11\Jean Disk Image\nps-2008-jean.E01. The Ignore orphan files in FAT file systems checkbox was left unchecked because the image is NTFS. Critically - and this is the most important configuration step of the entire week - the Time zone dropdown was set to (GMT+0:00) UTC before clicking Next. The task brief anchor 2008-07-20 01:28:03 is supplied in UTC, and the data source timezone must match for the Timeline Editor's GMT/UTC display mode and the keyword/time-window filters in Part C to produce correct hits.

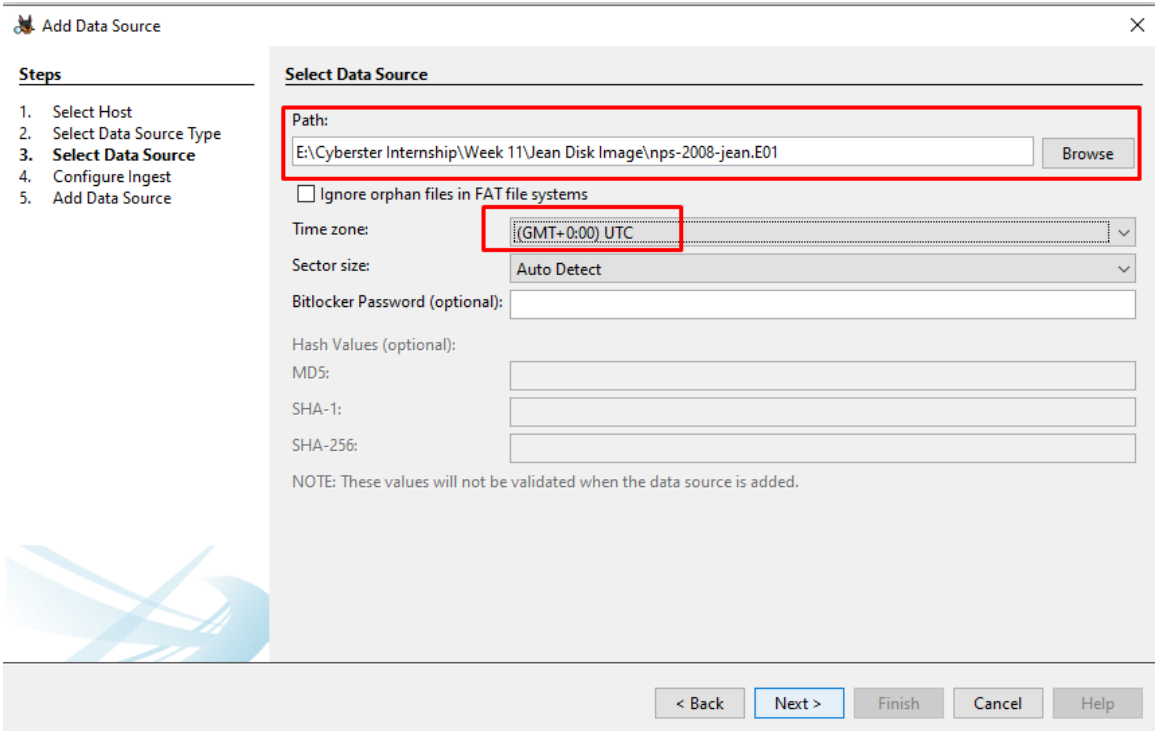


Fig 11.4 - Add Data Source wizard, step 3 of 5. Path: E:\Cyberster Internship\Week 11\Jean Disk Image\nps-2008-jean.E01. Time zone set to (GMT+0:00) UTC (red-boxed). Sector size: Auto Detect.

Phase 4 - Global Keyword Search Settings (m57plan)

Before clicking Next on the ingest configuration page, the Global Settings button on the Keyword Search module was opened so a case-specific keyword list could be defined. A new keyword list named Jean was created and a single keyword m57plan was added with the Keyword Type set to Exact Match. The Send ingest inbox messages for each hit checkbox was left enabled so any m57plan hit would surface in real time during ingest rather than only after completion.

Fig 11.5 - Autopsy Global Keyword Search Settings. Keyword list "Jean" created with a single keyword m57plan (Exact Match). Send ingest inbox messages for each hit: enabled.

Phase 5 - Configure Ingest Modules

Step 4 of 5 of the Add Data Source wizard is the Configure Ingest screen. Run ingest modules on was left at All Files, Directories, and Unallocated Space. The following modules were enabled:

- Recent Activity - populates Run Programs, USB Devices, Recent Documents, Shell Bags, Web Cookies, Web History.
- Hash Lookup - configured with a single MD5 hashset containing e23a4eb7f2562f53e88c9dca8b26a153 (the instructor-supplied target hash) for automatic flagging of m57biz.xls.
- File Type Identification - drives Extension Mismatch and downstream Picture Analyzer.
- Extension Mismatch Detector - surfaces files whose container header does not match their extension.
- Embedded File Extractor - unpacks archive content so Email Parser can index .eml / .msg inside .pst.
- Picture Analyzer - runs EXIF extraction; not directly relevant to Week 11 but cheap to enable.
- Keyword Search - Jean list (m57plan, Exact Match) plus the built-in IP Addresses / Email Addresses / Phone Numbers lists.
- Email Parser - parses .pst / .ost / .mbox / .eml; this is the module that surfaces outlook.pst as the email archive.
- Encryption Detection - flags Bitlocker / TrueCrypt / Office password-protected files (none expected in this case).
- Interesting Files Identifier - built-in suspicious filename / path rules.

PhotoRec Carver and Virtual Machine Extractor were left disabled to keep ingest time bounded. Add text to Solr Index was enabled (this is what makes the Keyword Search results queryable interactively after ingest, not just during ingest).

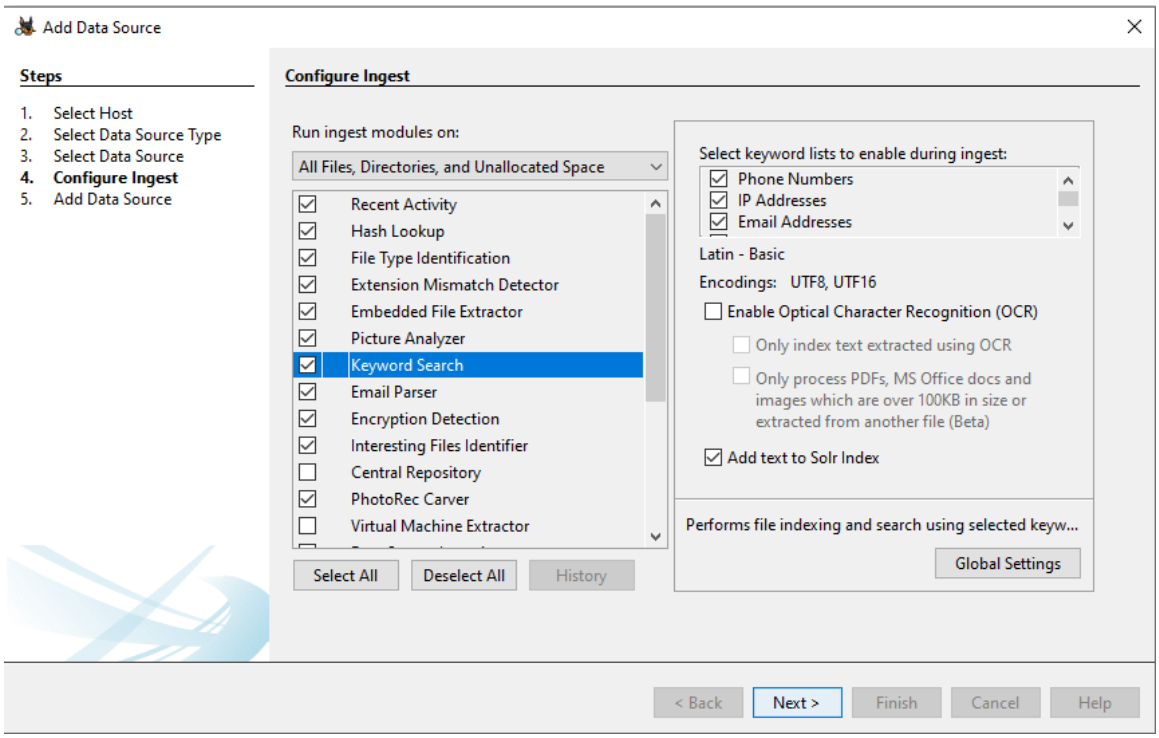


Fig 11.6 - Autopsy Configure Ingest screen. Ten modules enabled including Email Parser, Keyword Search with the Jean list, Recent Activity, and Embedded File Extractor. Add text to Solr Index: enabled.

On clicking Next and then Finish the data source was added and ingest started. Autopsy was left running uninterrupted for approximately 25 minutes while the modules executed sequentially. The Ingest Inbox surfaced m57plan keyword hits and a steady stream of E-Mail Messages parsed from outlook.pst during the second half of the run.

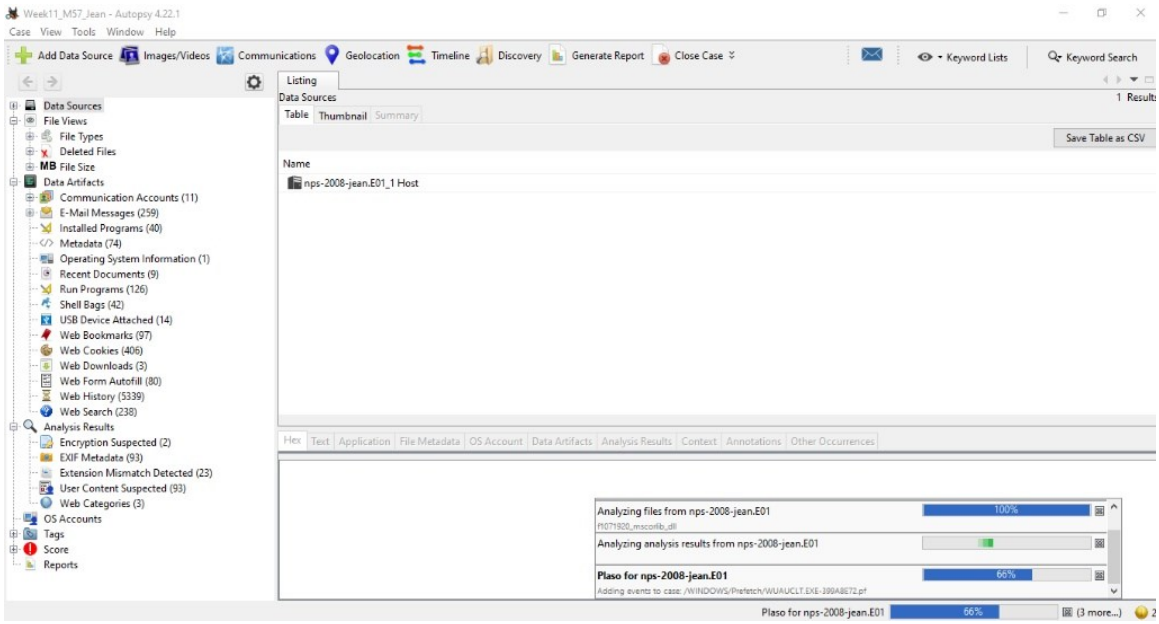


Fig 11.7 - Autopsy main window during ingest. Left panel populated with Data Sources, File Views, Data Artifacts (E-Mail Messages: 259 in this mid-ingest screenshot, growing to 261 by completion; Installed Programs: 40; Recent Documents: 9; Run Programs: 126; Web History: 5,339). Bottom-right progress bar shows the Plaso event ingestion stage at 66 percent - Plaso events for Part C are being added to the case automatically.

Phase 6 - Data Source Verification (MD5 Anchor)

After ingest completed, the Data Source Integrity Module result was opened by selecting the nps-2008-jean.E01 data source in the tree and reading the Analysis Results tab.

Evidence: Result: verified. MD5 hash verified - Calculated hash 78a52b5bac78f4e711607707ac0e3f93, Stored hash 78a52b5bac78f4e711607707ac0e3f93.

Interpretation: The on-disk E01 has not been modified since acquisition; Autopsy is reading the same bytes the instructor packaged. Any forensic conclusion drawn from this image is reproducible by any examiner with the same E01/E02 pair.

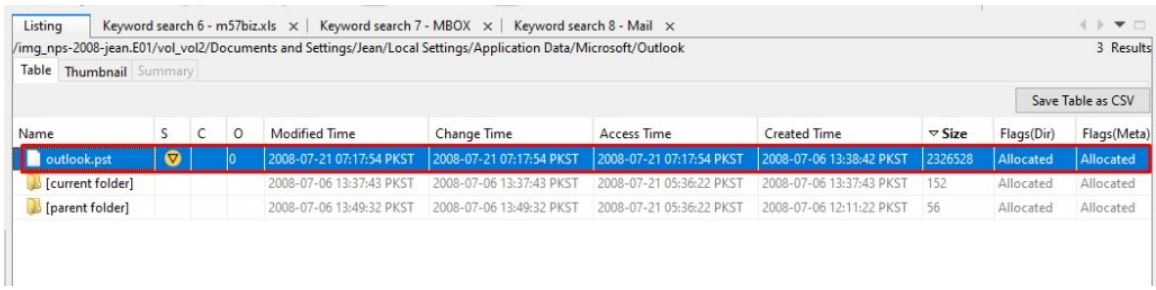


Fig 11.8 - Autopsy Data Source Verification Results for nps-2008-jean.E01. Result: verified. MD5 hash verified - Calculated: 78a52b5bac78f4e711607707ac0e3f93, Stored: 78a52b5bac78f4e711607707ac0e3f93.

Phase 7 - Locating Jean's Email Archive (outlook.pst)

Step 1: Initial Thunderbird hypothesis (negative)

The first hypothesis was that Jean's mail client would be Mozilla Thunderbird (MBOX format under Application Data\Thunderbird\Profiles\). Browsing Documents and Settings\Jean\Application Data\ in Autopsy produced no Thunderbird subdirectory. Four alternative search strategies were attempted in sequence - keyword search for *.msf files, browsing Local Settings\Application Data\ for a Thunderbird subdirectory there, filtering Views -> File Types -> By Extension for .msf, and confirming the exact casing of the username under Documents and Settings\. None returned a Thunderbird artefact, which rules out Thunderbird as the mail client.

Step 2: Pivot to Microsoft Outlook

The Keyword search 8 - Mail tab in Autopsy was opened. The path img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/Local Settings/Application Data/Microsoft/Outlook/ surfaces a single allocated file outlook.pst (2,326,528 bytes). Microsoft Outlook 2000 was Jean's mail client.

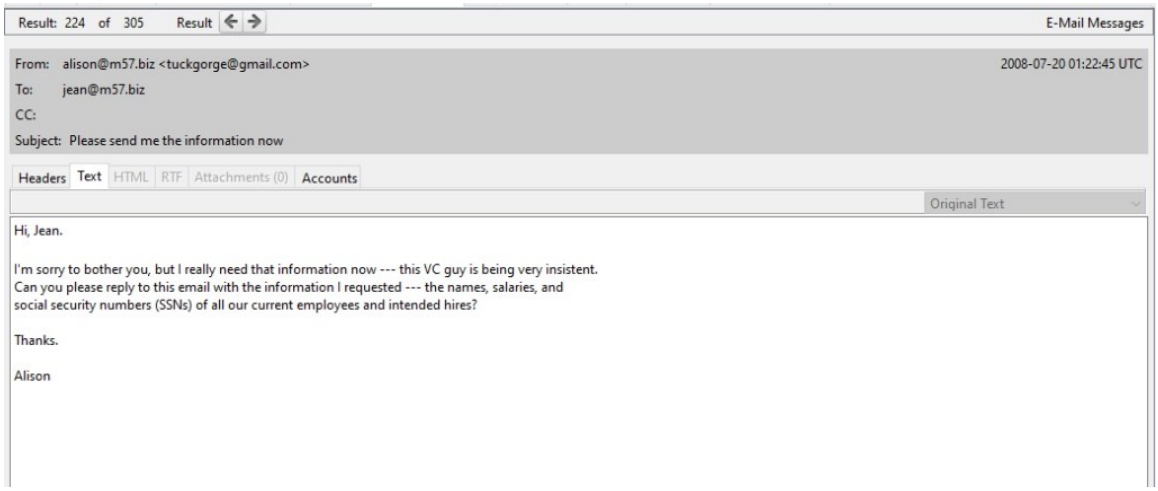


Fig 11.9 - Autopsy file browser at vol_vol2/Documents and Settings/Jean/Local Settings/Application Data/Microsoft/Outlook. outlook.pst (2,326,528 bytes) highlighted with a red box. Flags(Dir): Allocated. Flags(Meta): Allocated. This is Jean's email archive in Microsoft Outlook 2000 PST format. (Note: the Modified / Change / Access / Created Time columns in Autopsy's file-browser pane render in the examiner workstation's local timezone, not UTC; see the Methodology section for the read-protocol used to derive the UTC equivalents from tool-level UTC outputs.)

Autopsy's Email Parser module had already enumerated this PST during ingest. No manual export with a dedicated PST viewer was needed for primary triage; the parsed messages were available immediately under Results -> E-Mail Messages.

Phase 8 - Email Messages Triage in Autopsy

Result-count terminology used below

Autopsy reports two distinct counts that are easy to conflate. They are defined once here:

- 261 parsed email artefacts: the number of RFC 2822 messages that Autopsy's Email Parser successfully extracted from outlook.pst and inserted into the Data Artifacts -> E-Mail Messages -> Default folder. This is the count rendered as Default (261) in the left tree.
- 305 result navigation index: the total cursor-navigation count of the Result navigation row at the bottom of an individual E-Mail Messages selection view (visible as Result 261 of 305 or Result 223 of 305 in the screenshots that follow). This index includes the parsed 261 default-folder messages plus subviews and search-hit indices that Autopsy renders into the cursor. The 305 number is a UI navigation artefact and does not represent a separate evidentiary count.

The two counts are presented in the captions below exactly as they appear on screen, and are not relied upon as independent evidentiary numbers.

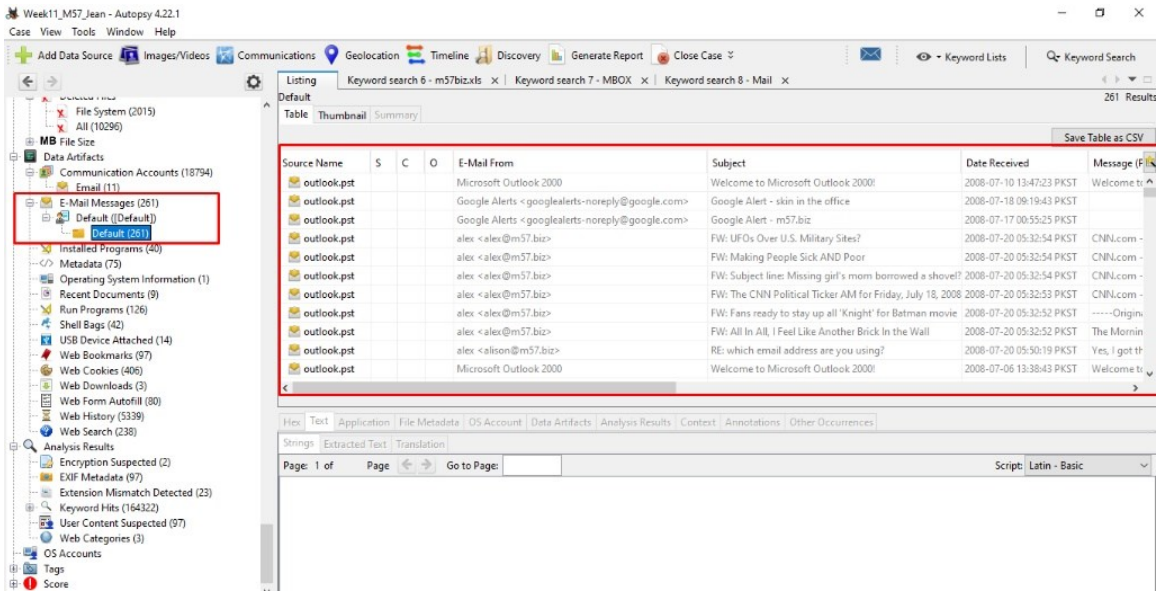
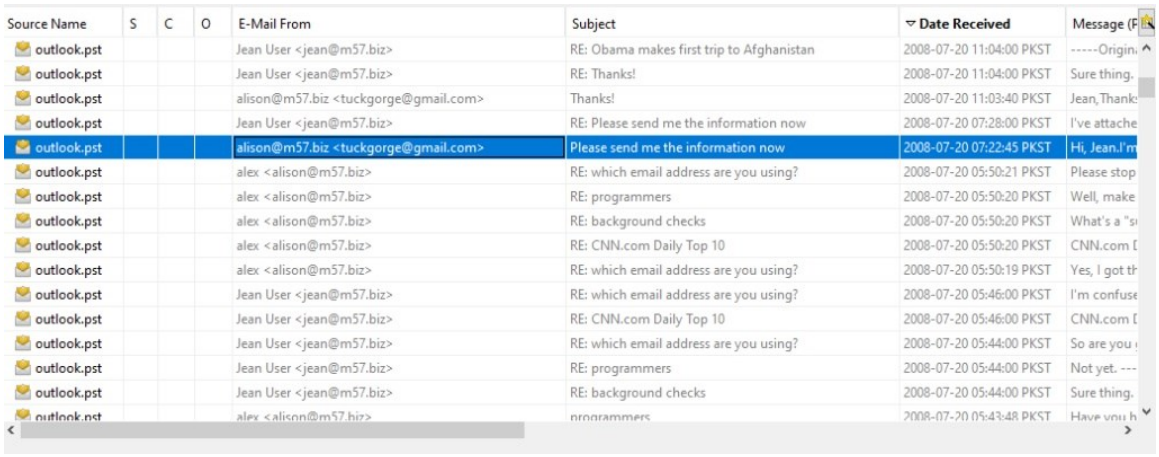


Fig 11.10 - Autopsy main window with Data Artifacts -> E-Mail Messages -> Default (261) selected in the left tree. Source Name column shows outlook.pst on every visible row. Subjects span Microsoft Outlook 2000 welcome, Google Alert traffic, and the long alex<alison@m57.biz> social-forward thread.

Sorting by Date Received and scrolling to 2008-07-20 reveals the relevant cluster. The decisive rows are listed in Phase 13's day-wide table; the bold row in that table is the email Jean physically sent with m57biz.xls attached.



Source Name	S	C	O	E-Mail From	Subject	Date Received	Message (F
outlook.pst				Jean User <jean@m57.biz>	RE: Obama makes first trip to Afghanistan	2008-07-20 11:04:00 PKST	-----Origin
outlook.pst				Jean User <jean@m57.biz>	RE: Thanks!	2008-07-20 11:04:00 PKST	Sure thing.
outlook.pst				alison@m57.biz <tuckgorge@gmail.com>	Thanks!	2008-07-20 11:03:40 PKST	Jean,Thank
outlook.pst				Jean User <jean@m57.biz>	RE: Please send me the information now	2008-07-20 07:28:00 PKST	I've attache
outlook.pst				alison@m57.biz <tuckgorge@gmail.com>	Please send me the information now	2008-07-20 07:22:45 PKST	Hi, Jean.I'm
outlook.pst				alex <alison@m57.biz>	RE: which email address are you using?	2008-07-20 05:50:21 PKST	Please stop
outlook.pst				alex <alison@m57.biz>	RE: programmers	2008-07-20 05:50:20 PKST	Well, make
outlook.pst				alex <alison@m57.biz>	RE: background checks	2008-07-20 05:50:20 PKST	What's a "s
outlook.pst				alex <alison@m57.biz>	RE: CNN.com Daily Top 10	2008-07-20 05:50:20 PKST	CNN.com [
outlook.pst				alex <alison@m57.biz>	RE: which email address are you using?	2008-07-20 05:50:19 PKST	Yes, I got th
outlook.pst				Jean User <jean@m57.biz>	RE: which email address are you using?	2008-07-20 05:46:00 PKST	I'm confuse
outlook.pst				Jean User <jean@m57.biz>	RE: CNN.com Daily Top 10	2008-07-20 05:46:00 PKST	CNN.com [
outlook.pst				Jean User <jean@m57.biz>	RE: which email address are you using?	2008-07-20 05:44:00 PKST	So are you
outlook.pst				Jean User <jean@m57.biz>	RE: programmers	2008-07-20 05:44:00 PKST	Not yet. ---
outlook.pst				Jean User <jean@m57.biz>	RE: background checks	2008-07-20 05:44:00 PKST	Sure thing.
outlook.pst				alex <alison@m57.biz>	programmers	2008-07-20 05:43:48 PKST	Have you h

Fig 11.11 - Autopsy E-Mail Messages, July 20 cluster. The selected (blue-highlighted) row is the inbound Please send me the information now request from alison@m57.biz <tuckgorge@gmail.com>. Other visible rows include Jean's outbound RE: Please send me the information now reply, the alison@m57.biz <tuckgorge@gmail.com> Thanks! follow-up, and the unrelated benign alex<alison@m57.biz> social-forward thread (programmers, background checks, CNN.com Daily Top 10, which email address are you using?).

Phase 9 - The Pivot Email: RE: Please send me the information now

Evidence: The outbound reply RE: Please send me the information now is selected in the E-Mail Messages view. The parsed metadata pane shows the following fields:

Field	Parsed Value
Date sent (Autopsy header)	2008-07-20 01:28:00 UTC
From (display + address)	Jean User <jean@m57.biz>
To (parsed display string)	alison@m57.biz
CC	(empty)
Subject	RE: Please send me the information now
Attachments (count)	1
Attachment filename	m57biz.xls
Attachment size (bytes)	291,840
Attachment MIME type	application/vnd.ms-excel
Attachment location in PST	/img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/Local Settings/Application Data/Microsoft/Outlook/outlook.pst/m57biz.xls
E-Mail Messages cursor index	Result 261 of 305 (UI navigation index; see Phase 8 disambiguation)

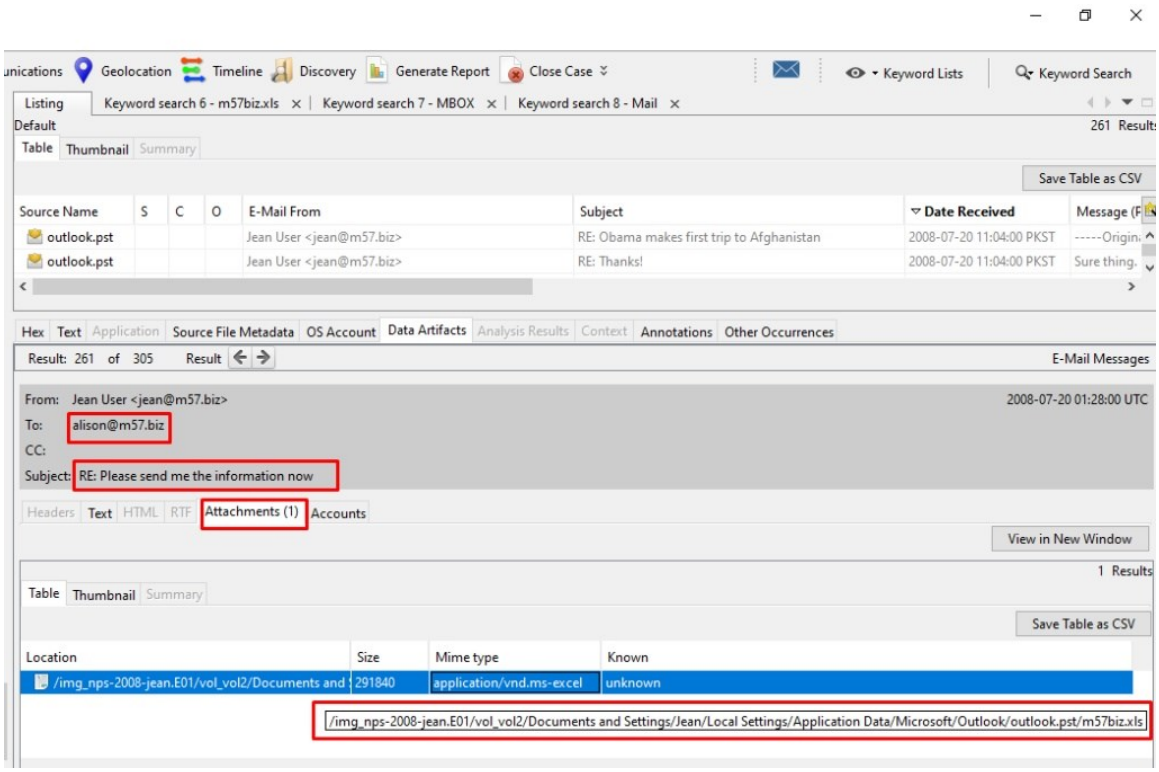


Fig 11.12 - Autopsy parsed view of the pivot email. From: Jean User <jean@m57.biz>; To: alison@m57.biz (red-boxed); Subject: RE: Please send me the information now (red-boxed). The Attachments (1) tab is highlighted. The attachment Location column ends in /m57biz.xls. Mime type: application/vnd.ms-excel. Size: 291,840 bytes.

Interpretation: On its face the parsed view is innocuous: Jean appears to have replied to alison@m57.biz with the spreadsheet attached. To recover the underlying reply address actually used by Outlook when Jean clicked Reply, the raw message body (which contains the quoted Original Message block of the inbound trigger) must be inspected via the Text tab.

Limitation - Hash Lookup status: The Known column for the attachment row reads unknown in this view. Autopsy's Hash Lookup module did not produce a hashset match for the attachment during parsing. The reason cannot be conclusively determined from on-image evidence alone; possible explanations include the way the Email Parser presents the PST attachment object to the Hash Lookup module, container-level encoding of the embedded attachment relative to the standalone Desktop\m57biz.xls copy, or differences between the stored attachment object and the instructor-supplied reference hash. Recommended follow-up: extract outlook.pst\m57biz.xls manually and re-hash with certutil -hashfile to confirm.

Phase 10 - Raw Header / Body Analysis: Display Name vs Underlying Address

Clicking the Text tab in the lower Autopsy pane renders the raw RFC 2822 message body. The first lines of the body are the operator-supplied prologue followed by Outlook's auto-generated Original Message divider and the quoted source of the inbound message Jean was replying to.

Evidence: The first line of the quoted Original Message block reads From: alison@m57.biz [mailto:tuckgorge@gmail.com]. The display portion of the From line is alison@m57.biz; the underlying address contained inside the [mailto:...] handler is tuckgorge@gmail.com. These two values do not match.

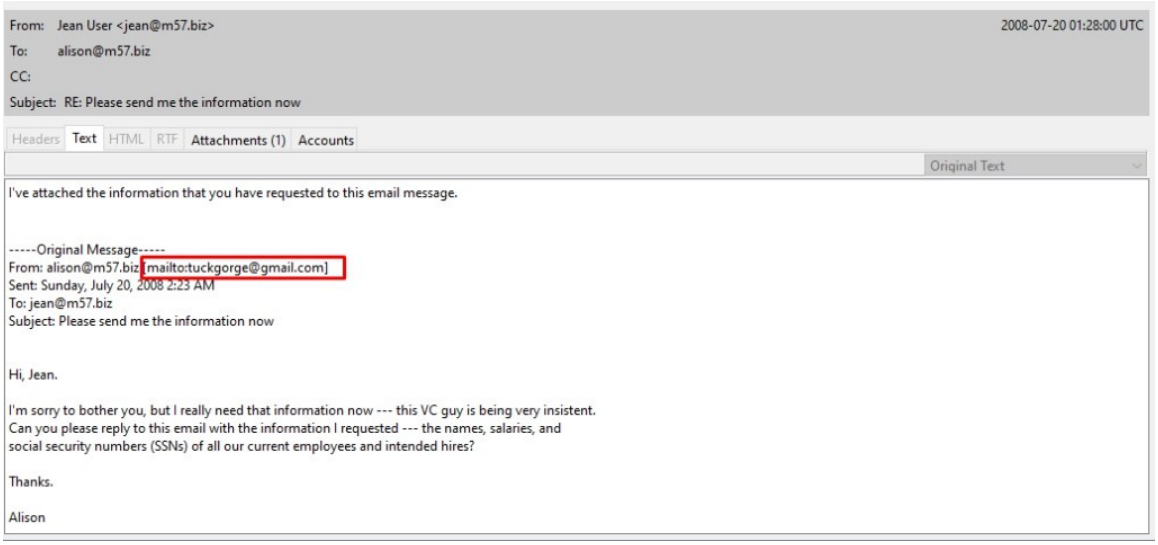


Fig 11.13 - Autopsy Text tab on the outbound pivot email. Body content with the Original Message block quoted. The red-boxed first line of the quoted block reads: From: alison@m57.biz [mailto:tuckgorge@gmail.com]. Sent: Sunday, July 20, 2008 2:23 AM. To: jean@m57.biz. Subject: Please send me the information now. The display portion (alison@m57.biz) and the underlying mailto address (tuckgorge@gmail.com) do not match. This is the central forensic finding of Part A.

Interpretation: Outlook 2000 constructs the To field of a reply using the underlying address associated with the original message rather than the display portion shown to the user. When Jean clicked Reply on the inbound Please send me the information now message, Outlook populated her reply envelope using the underlying tuckgorge@gmail.com value even though the display portion of the From line read alison@m57.biz. The effective reply recipient is therefore tuckgorge@gmail.com.

Limitation: This conclusion is drawn from the parsed PST contents and from documented Outlook reply behaviour. It is not corroborated by an independently captured SMTP envelope log, because no such log exists in this on-disk evidence set. Direct corroboration would require subpoena of the M57.biz MTA send logs (see D.4 recommended next steps). The on-image evidence is consistent with the underlying-address routing finding but does not by itself constitute SMTP envelope evidence.

Phase 11 - The Original Inbound Lure

Evidence: Result 223 of 305 (UI navigation index) in the same E-Mail Messages view is the inbound message Jean was replying to. The PST stored the From line with both the display portion and the underlying address surfaced; Autopsy's parser renders the From cell as alison@m57.biz <tuckgorge@gmail.com>. Subject: Please send me the information now (no RE prefix). Date received: 2008-07-20 01:22:45 UTC (4 minutes 18 seconds before Jean's reply).

Body of the inbound message (verbatim from Autopsy Text tab):

> Hi, Jean.
> I'm sorry to bother you, but I really need that information now --- this VC guy is being very insistent. Can you please reply to this email with the information I requested --- the names, salaries, and social security numbers (SSNs) of all our current employees and intended hires?
> Thanks.
> Alison

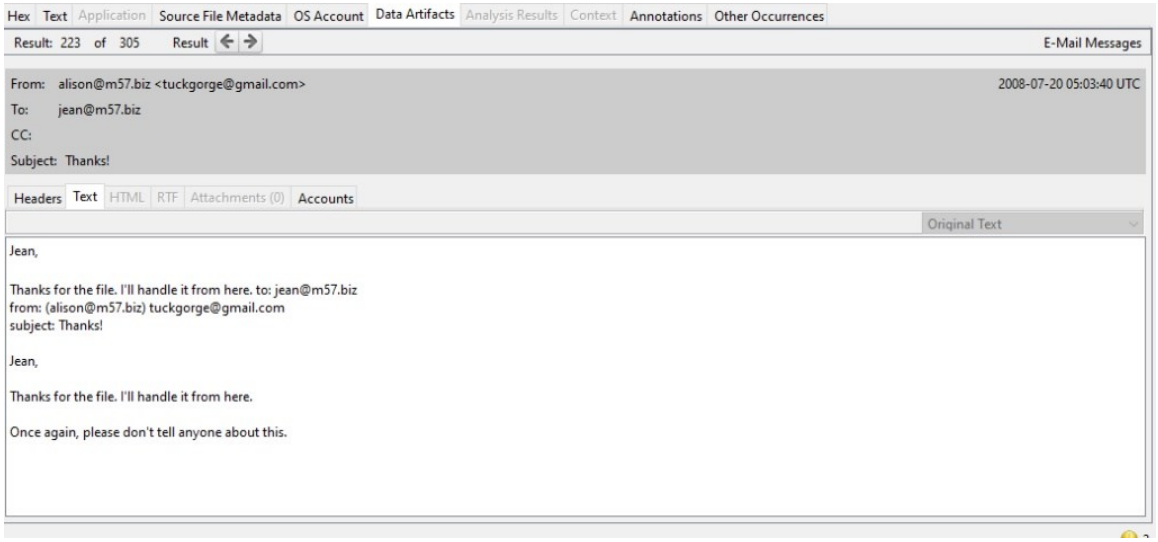


Fig 11.14 - Autopsy parsed view (Result 223 of 305) of the Thanks! follow-up acknowledgement from alison@m57.biz <tuckgorge@gmail.com>, Date Received 2008-07-20 05:03:40 UTC, addressed to jean@m57.biz. Body: "Jean, Thanks for the file. I'll handle it from here. Once again, please don't tell anyone about this."

Phase 12 - Recipient Acknowledgement: Thanks!

Evidence: Five hours and thirty-five minutes after Jean's reply, the same underlying-address identity sends a follow-up acknowledgement (Result 223 of 305 cursor index). Date Received: 2008-07-20 05:03:40 UTC. From: alison@m57.biz <tuckgorge@gmail.com> (Autopsy parser surfaces both components on this inbound message). To: jean@m57.biz. Subject: Thanks! Body: Jean, Thanks for the file. I'll handle it from here. Once again, please don't tell anyone about this.

Interpretation: The instruction "please don't tell anyone about this" is consistent with an external operator attempting to delay discovery of the data leak, and inconsistent with the language expected from a genuine internal request between the President and CFO of a company.

Limitation: The phrasing alone is not definitive proof of impersonation; it is one indicator alongside the underlying-address discrepancy. The strongest single piece of evidence remains the [mailto:tuckgorge@gmail.com] string in the original inbound message body (Fig 11.13).

Phase 13 - Day-Wide Communication Sweep (July 20, 2008)

All other emails on July 20, 2008 were reviewed for relevance. The full daily cluster contains the three operationally relevant messages described above plus benign personal traffic on two ongoing threads with alex <alison@m57.biz> - the separate, internal, lowercase-alex display identity discussed in the Identities section above. None of the benign traffic is anomalous; none reference m57biz.xls, m57plan, the company President in an authoritative capacity, or any third-party address.

Time (UTC)	Direction	From	To	Subject	Attachment
01:22:45	IN	alison@m57.biz <tuckgorge@gmail.com>	jean@m57.biz	Please send me the information now	-
01:28:00	OUT	Jean User <jean@m57.biz>	alison@m57.biz	RE: Please send me the information now	m57biz.xls (291,840 B)
05:03:40	IN	alison@m57.biz <tuckgorge@gmail.com>	jean@m57.biz	Thanks!	-
05:43:48	IN	alex <alison@m57.biz>	jean@m57.biz	programmers	-
05:44:00	IN	alex <alison@m57.biz>	jean@m57.biz	RE: background checks	-
05:46:00	IN	alex <alison@m57.biz>	jean@m57.biz	RE: CNN.com Daily Top 10	-
05:46:00	IN	alex <alison@m57.biz>	jean@m57.biz	RE: which email address are you using?	-
05:50:19	IN	alex <alison@m57.biz>	jean@m57.biz	RE: which email address are you using?	-
05:50:20	IN	alex <alison@m57.biz>	jean@m57.biz	RE: CNN.com Daily Top 10	-
05:50:21	IN	alex <alison@m57.biz>	jean@m57.biz	RE: programmers	-
05:50:21	IN	alex <alison@m57.biz>	jean@m57.biz	RE: background checks	-
05:50:21	IN	alex <alison@m57.biz>	jean@m57.biz	RE: which email address are you using?	-
11:03:40	OUT	Jean User <jean@m57.biz>	(alex thread)	Thanks!	-
11:04:00	OUT	Jean User <jean@m57.biz>	(alex thread)	RE: Thanks!	-
11:04:00	OUT	Jean User <jean@m57.biz>	(alex thread)	RE: Obama makes first trip to Afghanistan	-

Part A - Initial Conclusion (Email Evidence Only)

Based solely on the email evidence, Jean appears to have replied to an apparently internal request from alison@m57.biz and attached the requested spreadsheet (m57biz.xls, 291,840 bytes). The display portion on the inbound request was alison@m57.biz; the underlying address embedded in the [mailto:] handler of that inbound message was tuckgorge@gmail.com, a personal Gmail address. Outlook 2000 populates reply envelopes using the underlying address, so the effective reply recipient of Jean's outbound message is tuckgorge@gmail.com rather than the display portion alison@m57.biz. The same underlying-address identity sent a Thanks! follow-up 5 hours 35 minutes later, with language consistent with an external operator. Email evidence alone is therefore more consistent with a deceptive-request

scenario than with a deliberate internal exfiltration by Jean. Part B and Part C corroborate the on-host activity that produced this dispatch.

Part B - Host-Based Artefact Deep-Dive (Days 76-78)

Objective

Part B corroborates the email-side findings of Part A with three independent on-disk artefact categories - LNK, Prefetch, and Registry - each updated by a different Windows operating-system component in response to a discrete user action. If Jean opened m57biz.xls on the morning of July 20, 2008, all three categories should carry timestamps within seconds of each other and within seconds of the 01:28:03 UTC anchor.

Phase 14 - LNK File Extraction from Recent Folder

Evidence: Jean's Recent items folder at img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/Recent/ contains m57biz.lnk among other shortcut files. A second LNK exists at Application Data/Microsoft/Office/Recent/m57biz.LNK (the Office-MRU shortcut, distinct from the OS-level shortcut). Both point at the same target. The OS-level shortcut from Jean\Recent was extracted to C:\Forensics\Week11\Week11_M57_Jean\LNK\ via right-click -> Extract File(s).

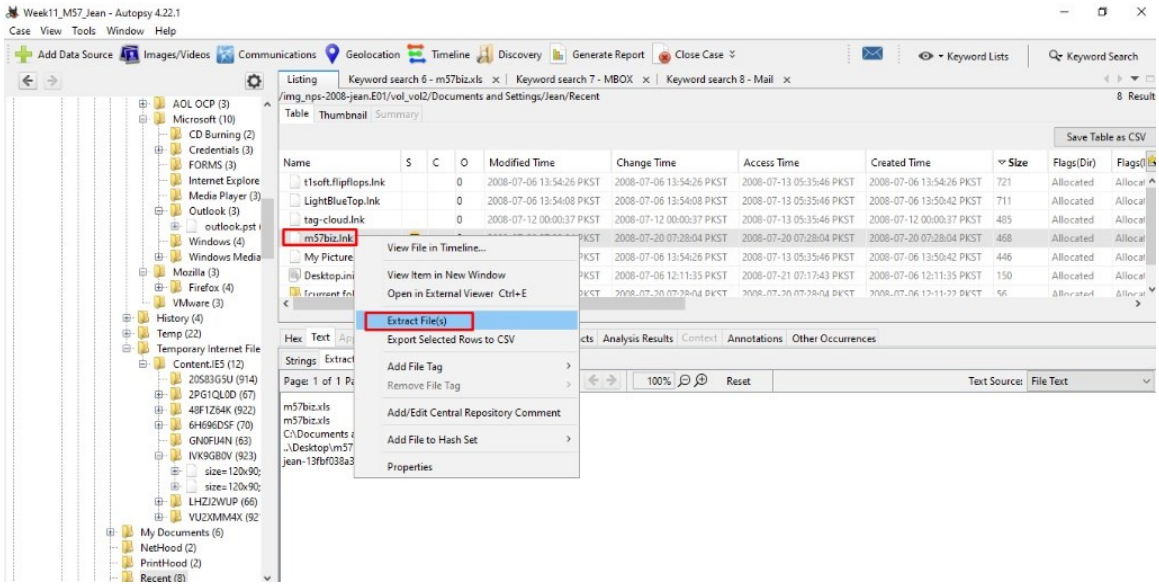


Fig 11.15 - Autopsy Recent directory listing for Jean. m57biz.lnk highlighted in red. Right-click context menu open with Extract File(s) highlighted. Other LNKs visible in the same directory: t1soft.flipflops.lnk, LightBlueTop.lnk, tag-cloud.lnk.

Phase 15 - LECmd Parse: m57biz.lnk (Header and Target Times)

From a Windows command prompt the extracted LNK was parsed with Eric Zimmerman's LECmd 2026.5.0:

C:\Forensics\Week11\Week11_M57_Jean\LNK\LECmd.exe -f "C:\Forensics\Week11\Week11_M57_Jean\LNK\m57biz.lnk" --csv "C:\Week11\LNK\Output" --dt "yyyy-MM-dd HH:mm:ss"

Evidence (top half of LECmd console): Target Created / Modified / Accessed: 2008-07-20 01:28:03 UTC (all three identical). File size: 291,840 bytes. Flags: HasTargetIdList, HasLinkInfo, HasRelativePath, HasWorkingDir, IsUnicode. File attributes: FileAttributeArchive. Show window: SwNormal. Relative Path: ..\Desktop\m57biz.xls. Working Directory: C:\Documents and Settings\Jean\Desktop.

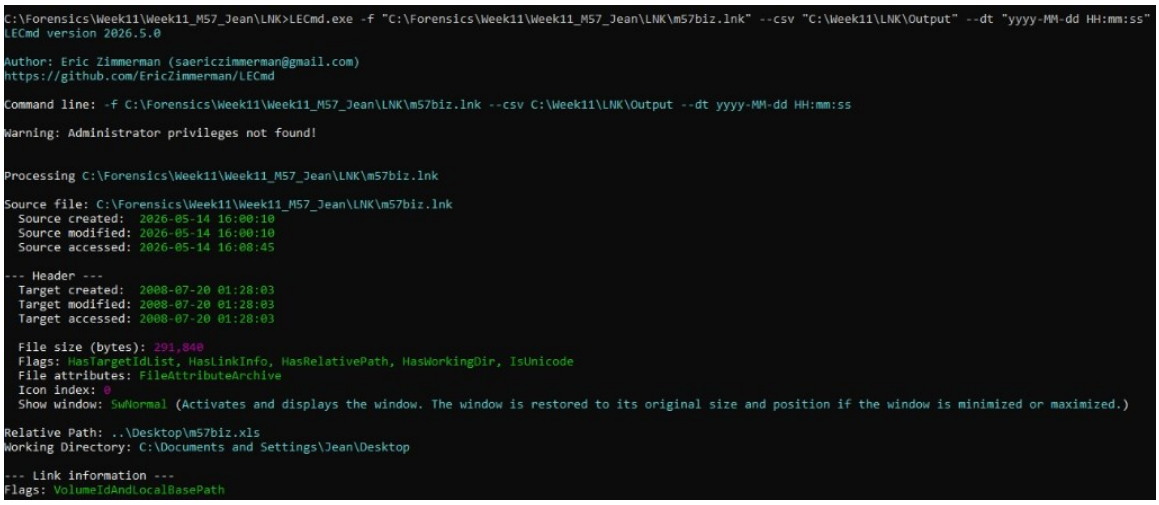


Fig 11.16 - LECmd 2026.5.0 console output, header and target-time block. Target created / modified / accessed (from the LNK header pointing at the original m57biz.xls): 2008-07-20 01:28:03 UTC (all three identical). File size: 291,840 bytes. Flags: HasTargetIdList, HasLinkInfo, HasRelativePath, HasWorkingDir, IsUnicode. Relative Path: ..\Desktop\m57biz.xls. Working Directory: C:\Documents and Settings\Jean\Desktop. (SourceCreated / Modified / Accessed lines at the top show the examiner workstation timestamps from when Autopsy extracted the file - these are not evidence of the original event.)

Phase 16 - LECmd Parse: Volume and Tracker Database Block

Evidence (bottom half of LECmd console): Drive type: Fixed storage media (Hard drive). Serial number: 744FC21F. Local path: C:\Documents and Settings\Jean\Desktop\m57biz.xls. Target ID (Beef0004) block: Long name m57biz.xls, Created 2008-07-20 01:28:04 UTC, Last access 2008-07-20 01:28:04 UTC. Tracker database block: Machine ID jean-13fbf038a3, MAC Address 00:0c:29:8d:35:2b, MAC Vendor VMWARE, Creation 2008-07-20 01:26:17 UTC. Extra blocks present: TrackerDataBaseBlock. Processing time: 0.388 seconds.

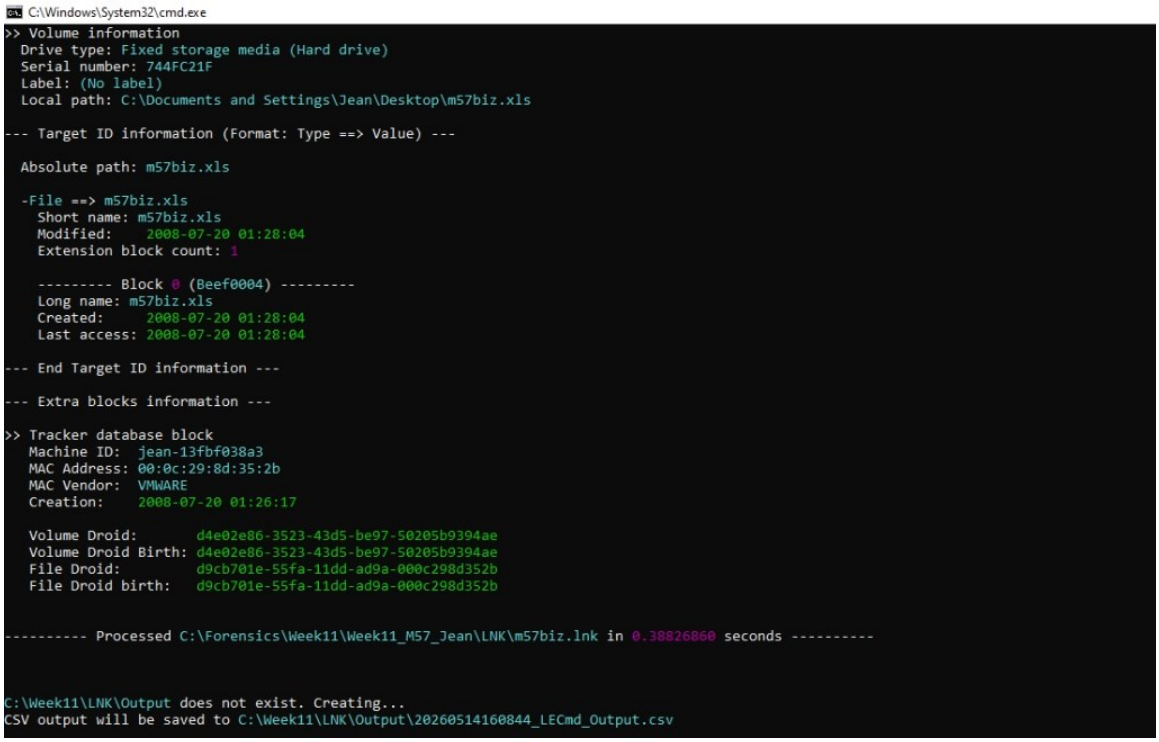


Fig 11.17 - LECmd Volume information and Tracker database block. Drive type: Fixed storage media (Hard drive). Serial number: 744FC21F. Local path: C:\Documents and Settings\Jean\Desktop\m57biz.xls. Target ID block (Beef0004) Long name m57biz.xls, Created / Last access 2008-07-20 01:28:04 UTC. Tracker database block: Machine ID jean-13fbf038a3, MAC Address 00:0c:29:8d:35:2b (VMware OUI), Creation 2008-07-20 01:26:17 UTC.

Interpretation: The Tracker block creation time 2008-07-20 01:26:17 UTC sits approximately 1 minute 46 seconds before the Target Modified timestamp 01:28:03 UTC. This represents the moment Windows created the Object Linking ID for the m57biz.xls reference (typically at first user-mode open), and the subsequent ~106 seconds represent Jean's in-application time before the final file write at 01:28:03. The MAC vendor VMware (OUI 00:0c:29) confirms the Jean workstation is a VMware virtual machine - consistent with Digital Corpora's packaging of the NPS m57 scenario.

Limitation: The Machine ID and MAC address bind this LNK to the named workstation jean-13fbf038a3 but do not bind it to a specific human operator beyond the user-account context (Jean's profile). Multi-user workstation scenarios cannot be ruled out from this artefact alone.

Phase 17 - LECmd CSV Inspection in Excel

The CSV written by LECmd (20260514160844_LECmd_Output.csv) was opened in Microsoft Excel. The spreadsheet contains a single data row with 28 columns. The full field dump is reproduced in Annex C.

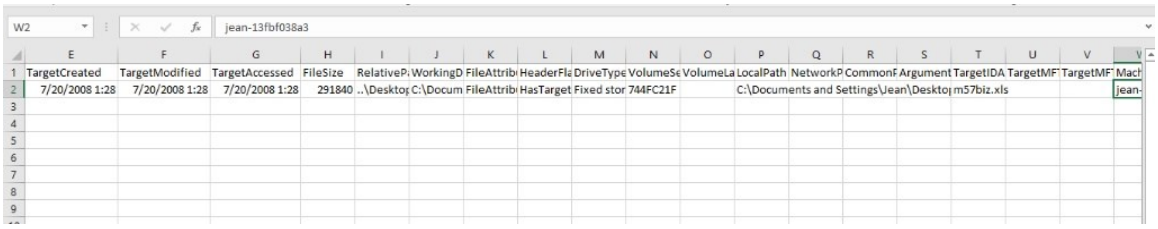


Fig 11.18 - 20260514160844_LECmd_Output.csv opened in Microsoft Excel. Cell W2 selected showing jean-13fbf038a3 in the MachineID column. Visible columns include TargetCreated, TargetModified, TargetAccessed (all 7/20/2008 1:28), FileSize (291840), RelativePath (..\Desktop\m57biz.xls), WorkingDirectory (C:\Documents and Settings\Jean\Desktop), VolumeSerialNumber (744FC21F), LocalPath (C:\Documents and Settings\Jean\Desktop\m57biz.xls), TargetIDAbsolutePath (m57biz.xls), MachineID (jean-13fbf038a3).

Phase 18 - Excel Prefetch Extraction (EXCEL.EXE-1C75F8D6.pf)

Evidence: The Prefetch directory at vol_vol2/WINDOWS/Prefetch/ contains 132 prefetch files. The EXCEL.EXE entry is EXCEL.EXE-1C75F8D6.pf (1C75F8D6 is Microsoft's 8-character path hash for C:\Program Files\Microsoft Office\Office\EXCEL.EXE on this Windows XP build). Right-click -> Extract File(s) saved the prefetch to C:\Forensics\Week11\Week11_M57_Jean\Prefetch\EXCEL.EXE-1C75F8D6.pf (30,510 bytes).

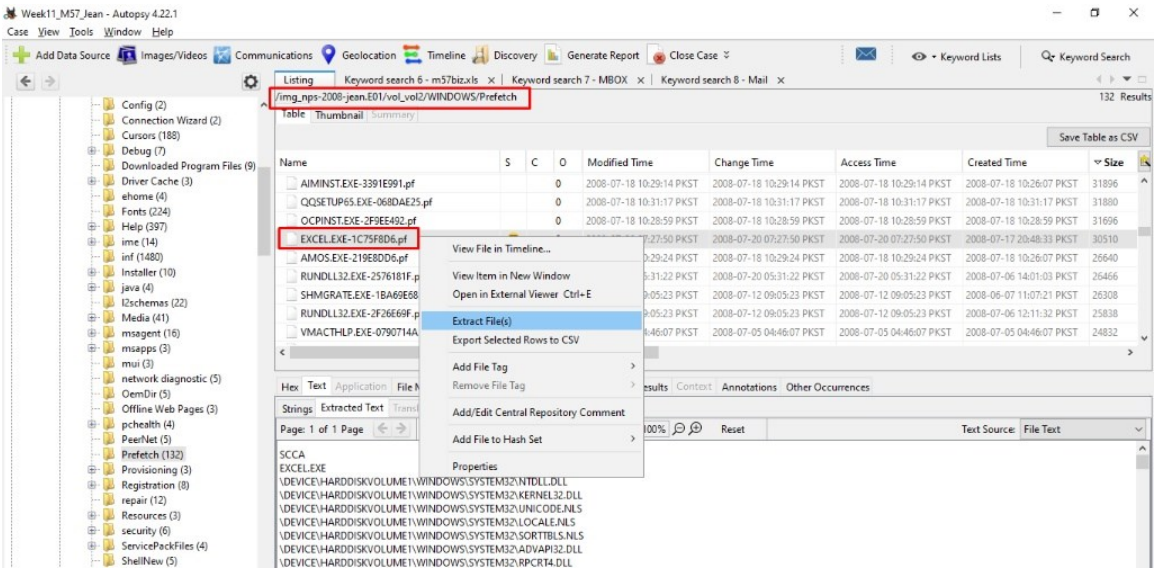


Fig 11.19 - Autopsy file browser at /img_nps-2008-jean.E01/vol_vol2/WINDOWS/Prefetch (132 results). EXCEL.EXE-1C75F8D6.pf highlighted in red. Right-click context menu open with Extract File(s) highlighted. The Extracted Text preview pane shows the standard SCCA header and the file references list starting with NTDLL.DLL, KERNEL32.DLL, UNICODE.NLS, LOCALE.NLS, SORTTBLS.NLS.

Phase 19 - PECmd Parse: Header, Run Count, Volume

The extracted prefetch was parsed with Eric Zimmerman's PECmd 2026.5.0:

C:\Forensics\Week11\Week11_M57_Jean\Prefetch>PECmd.exe -f "C:\Forensics\Week11\Week11_M57_Jean\Prefetch\EXCEL.EXE-1C75F8D6.pf" --csv "C:\Forensics\Week11\Weel11_M57_Jean\Prefetch\Output" --dt "yyyy-MM-dd HH:mm:ss"

Evidence (PECmd header block): Executable name: EXCEL.EXE. Hash: 1C75F8D6. File size: 30,510 bytes. Version: Windows XP or Windows Server 2003. Run count: 2. Last run: 2008-07-20 01:27:40 UTC. Volume0 name: \DEVICE\HARDDISKVOLUME1. Volume0 serial: 744FC21F (matches the LECmd Volume Serial - same disk). Volume0 created: 2008-05-13 22:18:43 UTC. Directories referenced: 31. File references: 91.

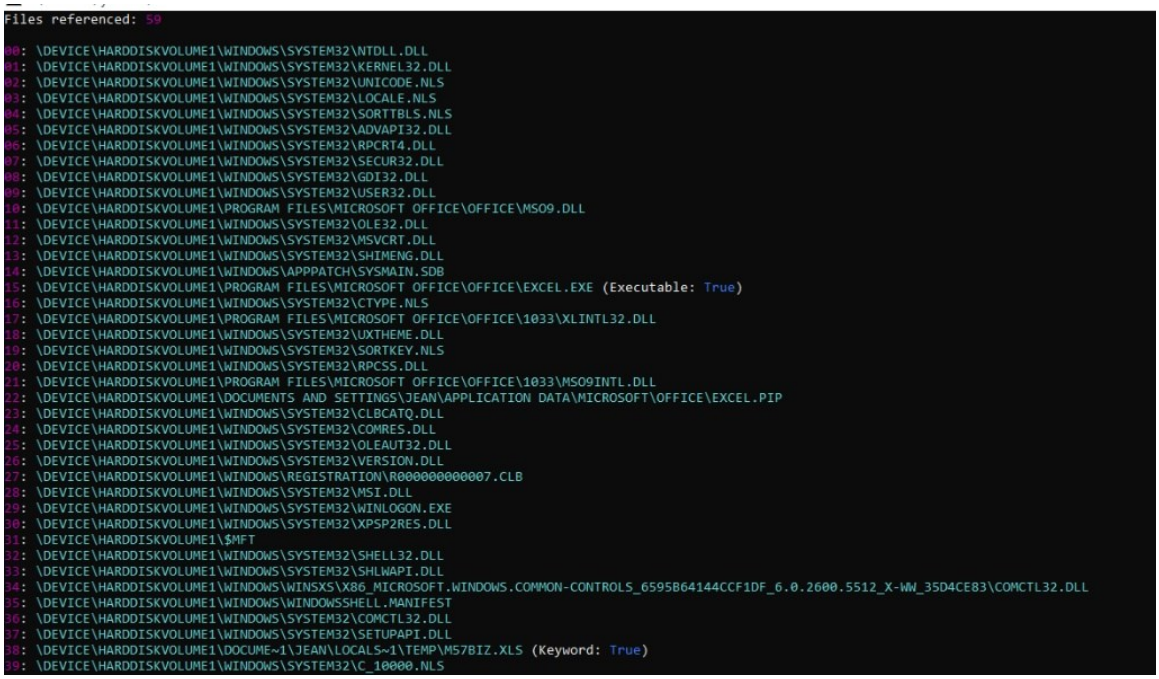


Fig 11.20 - PECmd 2026.5.0 console output, header block. Command line shown at top. Processing C:\Forensics\Week11\Week11_M57_Jean\Prefetch\EXCEL.EXE-1C75F8D6.pf. Executable name: EXCEL.EXE. Hash: 1C75F8D6. File size: 30,510 bytes. Version: Windows XP or Windows Server 2003. Run count: 2. Last run: 2008-07-20 01:27:40 UTC. Volume0 name \DEVICE\HARDDISKVOLUME1, Serial 744FC21F, Created 2008-05-13 22:18:43 UTC. Directories: 31. File references: 91.

Interpretation: The Last run 2008-07-20 01:27:40 UTC sits 23 seconds before the file Modified anchor 01:28:03 UTC. This is consistent with the moment the Windows XP cache manager triggered EXCEL.EXE's prefetch write as Jean's double-click on m57biz.xls handed off to Excel. The 23-second gap is consistent with normal Excel startup time on a 2008-era VM plus the time required for the user to briefly review the spreadsheet content before composing a reply.

Phase 20 - PECmd Parse: Files Referenced (Top Block)

The Files referenced block of the PECmd output lists 59 unique paths that EXCEL.EXE touched during its prefetch capture window. The first thirty entries are standard Windows XP boot-DLL load chain plus Excel's own dependencies.

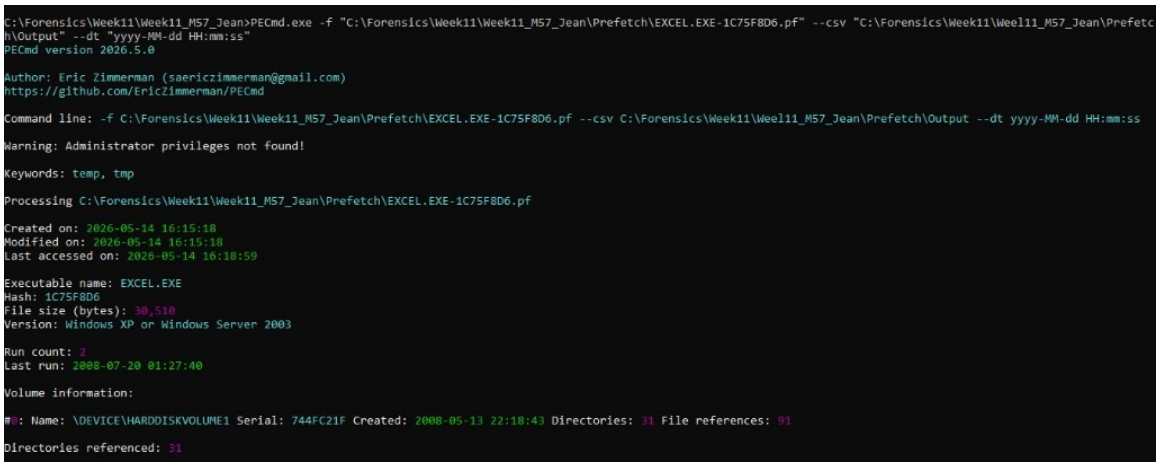


Fig 11.21 - PECmd Files Referenced block, top portion. Header line reads "Files referenced: 59". First entries show \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\NTDLL.DLL, KERNEL32.DLL, UNICODE.NLS, LOCALE.NLS, SORTTBLS.NLS, ADVAPI32.DLL, RPCRT4.DLL, SECUR32.DLL, GDI32.DLL, USER32.DLL, and at index 10 \DEVICE\HARDDISKVOLUME1\PROGRAM FILES\MICROSOFT OFFICE\OFFICE\MSO9.DLL. The presence of the Office MSO9.DLL and other Office-specific DLLs early in the list confirms the run is an Office application start.

Phase 21 - PECmd Parse: Files Referenced (Middle Block)

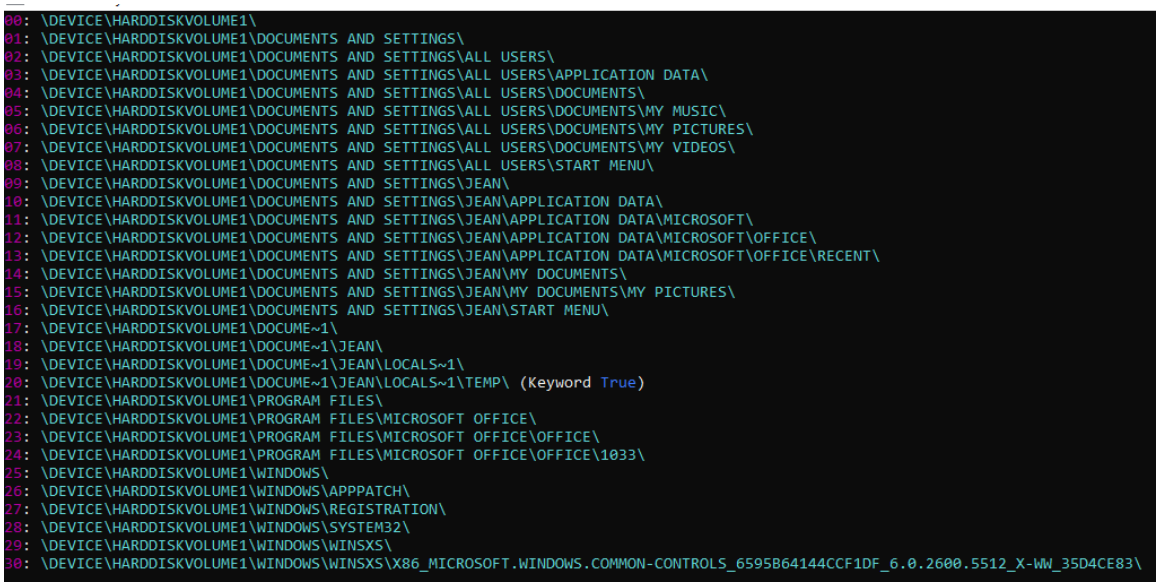


Fig 11.22 - PECmd Files Referenced block, middle portion (entries 00-30 visible in cyan). Index 09 \DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\JEAN\ (the user profile directory is touched as part of Excel's recent-files MRU population - confirms the run is by user Jean). Index 13 \DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\JEAN\APPLICATION DATA\MICROSOFT\OFFICE\RECENT\ (the Office MRU shortcut directory). Index 20 \DEVICE\HARDDISKVOLUME1\DOCUME~1\JEAN\LOCALS~1\TEMP\ (Keyword: True, the temp directory where Excel may stage the file).

Phase 22 - PECmd Parse: Files Referenced (m57biz.xls Confirmation)

Evidence (PECmd Files Referenced bottom block): Index 38 of the Files Referenced list reads \DEVICE\HARDDISKVOLUME1\DOCUME~1\JEAN\LOCALS~1\TEMP\M57BIZ.XLS (Keyword: True). Index 40 reads \DEVICE\HARDDISKVOLUME1\DOCUME~1\JEAN\LOCALS~1\TEMP\~DFF9E0.TMP (Keyword: True). Index 57 reads \DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\JEAN\APPLICATION DATA\MICROSOFT\OFFICE\RECENT\TEMP.LNK (Keyword: True). Processing time: 0.20902260 seconds.

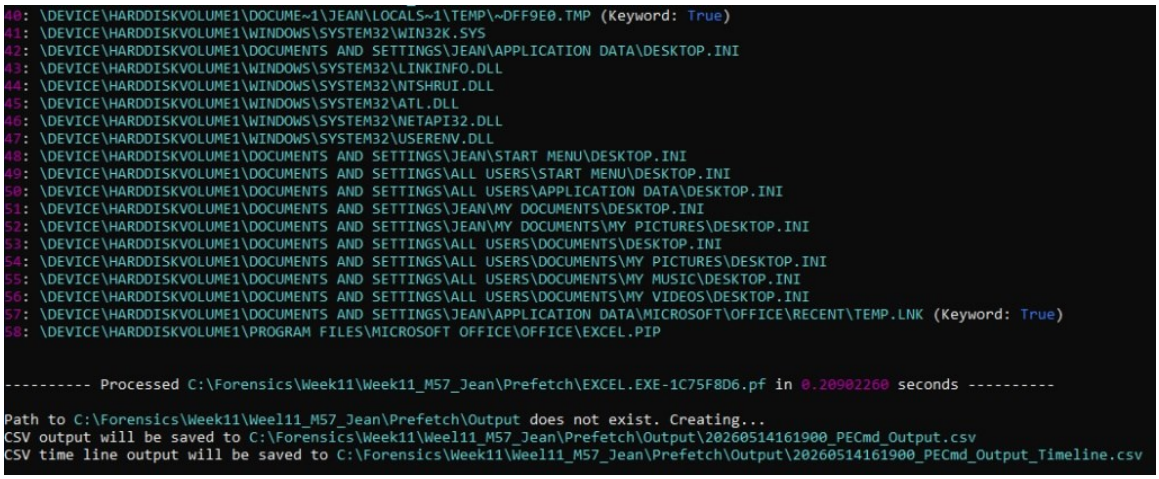


Fig 11.23 - PECmd Files Referenced block, bottom portion (entries 40-58 plus processing footer). Index 40 \DEVICE\HARDDISKVOLUME1\DOCUME~1\JEAN\LOCALS~1\TEMP\~DFF9E0.TMP (Keyword: True - Excel temp scratch file). Index 41 \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\WIN32K.SYS. Index 47 \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\USERENV.DLL. Index 57 \DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\JEAN\APPLICATION DATA\MICROSOFT\OFFICE\RECENT\TEMP.LNK (Keyword: True - the Office Recent folder shortcut being updated). Footer: Processed in 0.20902260 seconds, CSV output paths.

Interpretation: Index 38 (M57BIZ.XLS in Jean's user temp directory) is the operationally decisive entry in the Files Referenced list. It demonstrates - independently of the LNK timestamps and the registry RecentDocs key - that EXCEL.EXE on this run accessed a file named M57BIZ.XLS. The argument that the prefetch was written by some unrelated invocation of Excel is therefore not supported.

Summary of decisive Files Referenced rows (full list in Annex D):

Row #	Path	Forensic significance
15	\DEVICE\HARDDISKVOLUME1\PROGRAM FILES\MICROSOFT OFFICE\OFFICE\EXCEL.EXE	(Executable: True) - the executable itself
22	\DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\JEAN\APPLICATION DATA\MICROSOFT\OFFICE\EXCEL.PIP	Excel's per-user toolbar preference file - confirms the run was under Jean's user context
38	\DEVICE\HARDDISKVOLUME1\DOCUME~1\JEAN\LOCALS~1\TEMP\M57BIZ.XLS (Keyword: True)	Direct binding - Excel created or accessed a temporary copy of M57BIZ.XLS in Jean's local temp

		directory during this run
57	\DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\JEAN\APPLICATION DATA\MICROSOFT\OFFICE\RECENT\TEMP.LNK (Keyword: True)	Office MRU shortcut written/updated during the same run

Phase 23 - NTUSER.DAT Hive Extraction from Autopsy

Jean's NTUSER.DAT registry hive lives in the user profile root at vol_vol2/Documents and Settings/Jean/. NTUSER.DAT (786,432 bytes) was selected; its companion transaction log NTUSER.DAT.LOG (1,024 bytes) was extracted at the same time. Both files were saved to C:\Forensics\Week11\Week11_M57_Jean\Registry\.

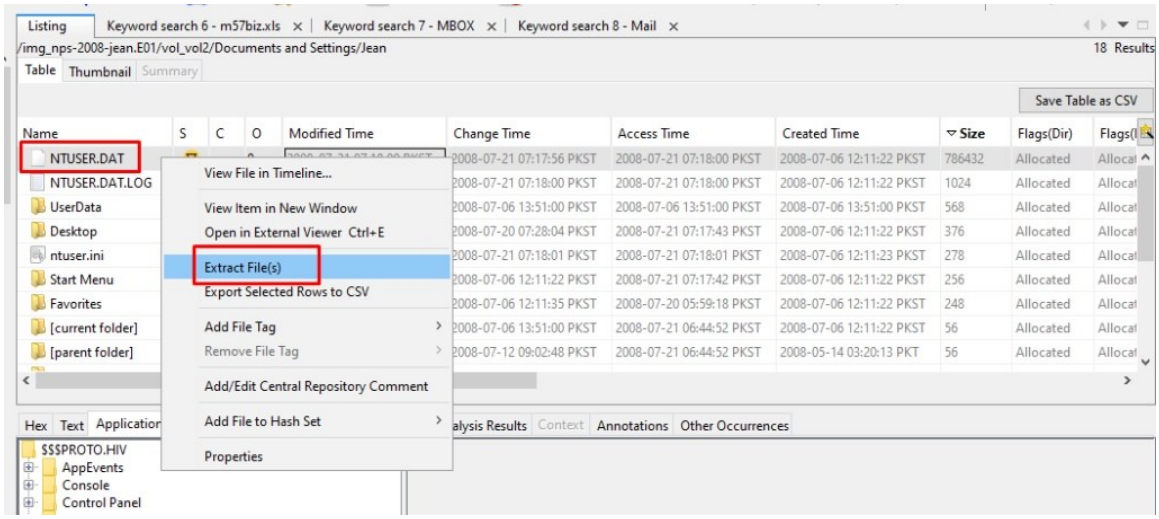


Fig 11.24 - Autopsy file browser at /img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean (18 results). NTUSER.DAT highlighted (red box). Right-click context menu open with Extract File(s) highlighted (red box). Other entries visible: NTUSER.DAT.LOG, UserData, Desktop, ntuser.ini, Start Menu, Favorites. The bottom-left Application pane previews the hive root keys $$$PROTO.HIV, AppEvents, Console, Control Panel - confirming a valid registry hive header.

Phase 24 - Registry Explorer: RecentDocs\.xls Subkey

Evidence: Registry Explorer 2026.5.0 was launched as Administrator and File -> Load Offline Hive -> NTUSER.DAT loaded the hive (with auto-detection of NTUSER.DAT.LOG). Navigation path: Software -> Microsoft -> Windows -> CurrentVersion -> Explorer -> RecentDocs. The .xls subkey is selected. Right pane Recent documents tab: Extension .xls, Value Name 0, Target Name m57biz.xls, Lnk Name m57biz.lnk, Mru Position 0, Opened On 2008-07-20 01:28:04 UTC. Last write timestamp on the .xls subkey: 2008-07-20 01:28:04 UTC. Total rows: 1.

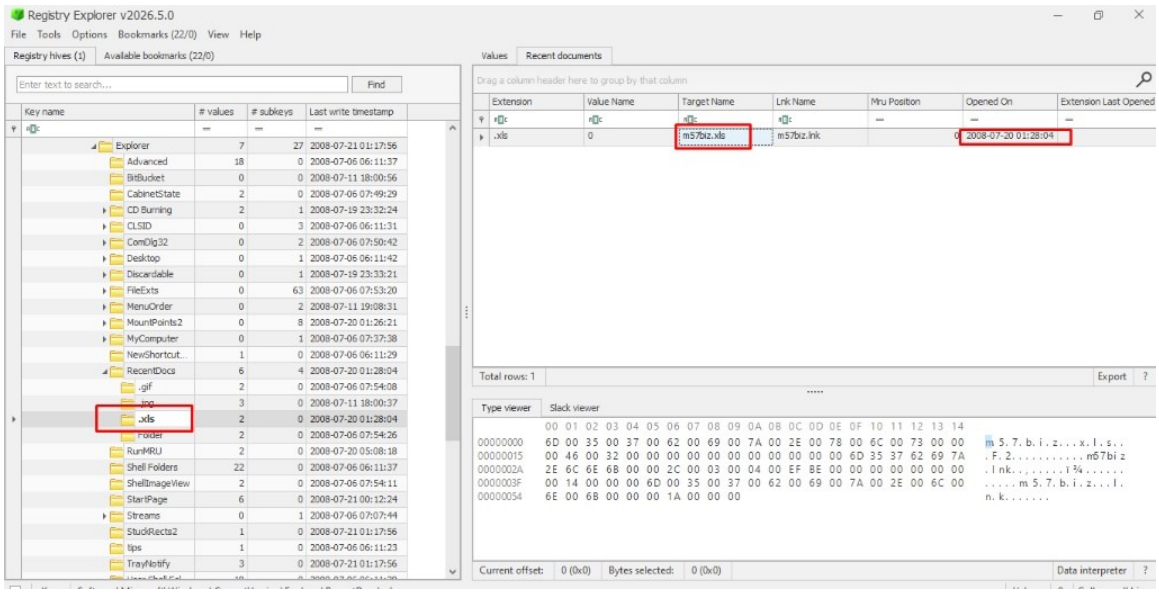


Fig 11.25 - Registry Explorer 2026.5.0 with NTUSER.DAT loaded. Left tree expanded to Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs; the .xls subkey is highlighted in red. Right pane Recent documents tab shows a single row: Extension .xls, Target Name m57biz.xls (red-boxed), Lnk Name m57biz.lnk, Opened On 2008-07-20 01:28:04 UTC (red-boxed). Last write timestamp on the .xls subkey: 2008-07-20 01:28:04 UTC. Type viewer hex pane visible at bottom showing the binary value 0 raw bytes decoding to "m57biz.xls...m57biz.lnk".

Interpretation: The .xls subkey has exactly one MRU entry. m57biz.xls is the only .xls file Jean has ever opened from Explorer or from any application that publishes recent-file events to the Windows shell. There is no competing or older .xls history. The subkey's last-write timestamp (2008-07-20 01:28:04 UTC) is one second after the LNK Target Modified timestamp (01:28:03) - the expected sequence (Explorer updates RecentDocs slightly after Excel writes the file in response to the open).

Phase 25 - Registry Explorer: Office\11.0\Excel\Recent Files

Evidence: Navigation path: Software -> Microsoft -> Office -> 11.0 -> Excel -> Recent Files. The Recent Files subkey is selected. Right pane Values tab: Value Name File1, Value Type RegSz, Data C:\Documents and Settings\Jean\Desktop\m57biz.xls. Last write timestamp on the Recent Files subkey: 2008-07-20 01:28:13 UTC.

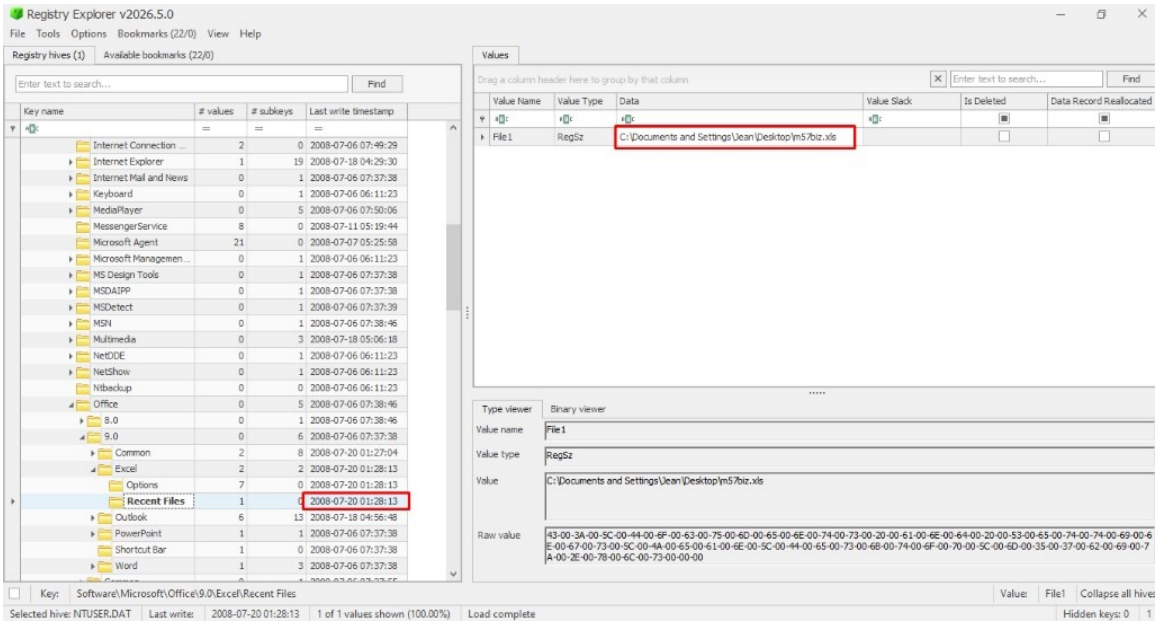


Fig 11.26 - Registry Explorer with NTUSER.DAT loaded, navigated to Software\Microsoft\Office\11.0\Excel\Recent Files. Right pane Values tab shows one row: Value Name File1, Value Type RegSz, Data C:\Documents and Settings\Jean\Desktop\m57biz.xls (red-boxed). Last write timestamp on the Recent Files subkey: 2008-07-20 01:28:13 UTC (red-boxed at bottom-left status bar - selected hive NTUSER.DAT, last write 2008-07-20 01:28:13).

Registry Subkey	Value	Data	Last Write (UTC)
...\Explorer\RecentDocs\.xls	0 (binary MRU)	Target Name m57biz.xls; Lnk Name m57biz.lnk	2008-07-20 01:28:04
...\Office\11.0\Excel\Recent Files	File1 (RegSz)	C:\Documents and Settings\Jean\Desktop\m57biz.xls	2008-07-20 01:28:13

Interpretation: The 9-second gap between the two registry writes (01:28:04 -> 01:28:13) is the characteristic gap between an Explorer-managed RecentDocs update (written immediately on file open) and an Office-managed Recent Files MRU update (written when Excel commits its own session state, typically after the document parse is complete). The two registry locations record two distinct stages of the same open event - additional internal-consistency evidence that the open is real and not synthesised.

Phase 26 - Three-Artefact Corroboration Table

Artefact category	Full path in image (or registry path)	Timestamp (UTC)	User action represented
LNK Target Created / Modified / Accessed	vol_vol2\Documents and Settings\Jean\Recent\m57biz.lnk -> Desktop\m57biz.xls	2008-07-20 01:28:03	OS recorded the moment m57biz.xls became the target recent-items shortcut
LNK Target ID block Long name Created / Last access	(same)	2008-07-20 01:28:04	Shell item creation event rec inside the LNK target-ID struc

LNK Tracker block Creation	(same)	2008-07-20 01:26:17	First Object Linking ID genera for this target reference
Excel Prefetch Last Run	vol_vol2\WINDOWS\Prefetch\EXCEL.EXE-1C75F8D6.pf	2008-07-20 01:27:40	Kernel-level record of EXCEL. process start by user Jean
Excel Prefetch Files Referenced row 38	\DEVICE\HARDDISKVOLUME1\DOCUME~1\JEAN\LOCALS~1\TEMP\M57BIZ.XLS	(within same run)	Excel touched M57BIZ.XLS in temp directory during the 01:27:40 run
Registry RecentDocs\.xls last write	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.xls	2008-07-20 01:28:04	Explorer-managed OS recent-documents MRU update
Registry Office\11.0\Excel\Recent Files last write	NTUSER.DAT\Software\Microsoft\Office\11.0\Excel\Recent Files	2008-07-20 01:28:13	Excel 2003-managed applicat level recent-files MRU update
Email outbound dispatch (cross-reference to Part A)	outlook.pst -> Sent Items -> RE: Please send me the information now	2008-07-20 01:28:00	Outlook 2000 wrote the outb message including m57biz.xls attachment to the PST send q

Part B verdict: The three on-disk artefact categories (LNK, Prefetch, Registry) plus the PST-store cross-reference cluster within 33 seconds of each other (01:27:40 prefetch-run through 01:28:13 last MRU write) and are mutually consistent. Jean's account at the host level - that she opened the file in Excel and replied to alison@m57.biz with it attached - is corroborated by the host artefacts. The Part A discrepancy in the underlying address of the inbound lure remains the analytic pivot.

Part C - Super Timeline Analysis (Days 79-80)

Objective

Part C generates a system-wide super timeline of every dated artefact on the image and applies progressive filtering (date -> time-window -> keyword) to collapse the unfiltered timeline into a minimal sequence of events that demonstrates the second-by-second flow of activity inside the investigation window. The Start Big - Filter Down methodology from the task brief is observed in full, and each filter stage's event count is explicitly recorded for validation.

Phase 27 - Generating the Autopsy Timeline

Autopsy's built-in Timeline tool was used (Tools -> Timeline). Because Plaso ingest had already run during the original Add Data Source pass, the timeline appeared within a few seconds of the Timeline window opening; no separate log2timeline invocation was needed.

Stage 1 event count - unfiltered: The unfiltered timeline contains all Plaso-indexed events across the full image - approximately one million events spanning the 1970 UNIX epoch (a single artefact whose timestamp was lost) through the image acquisition date in 2008. The Counts view (Logarithmic scale) renders the bulk of activity across 1996-2008 as expected for a Windows XP user-profile image.

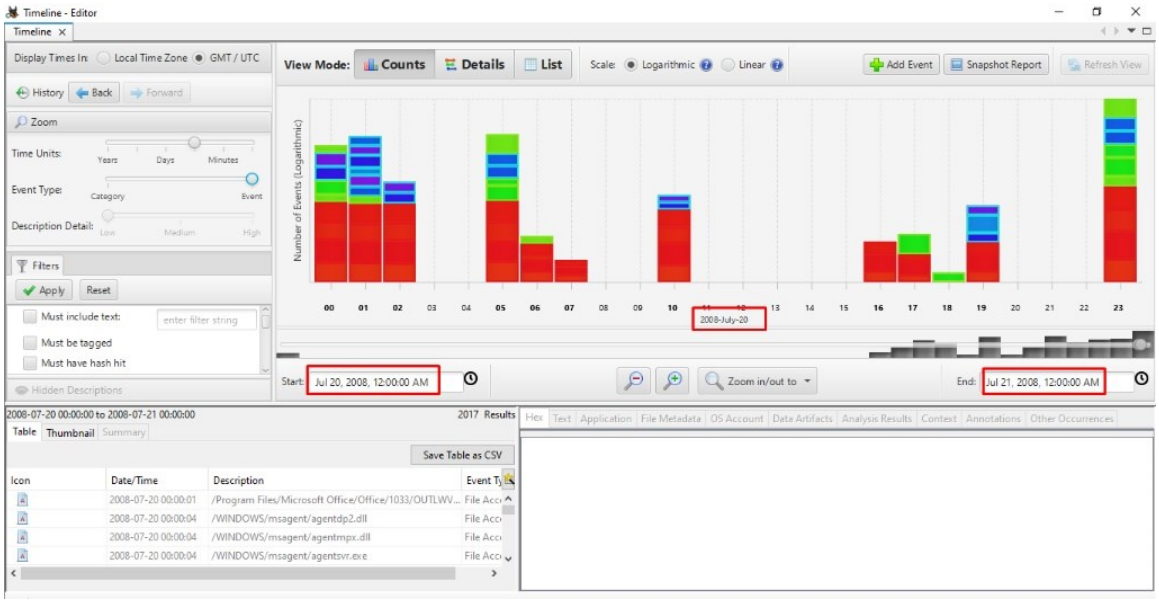


Fig 11.27 - Autopsy Timeline Editor, Counts view, Logarithmic scale, full unfiltered timeline. Time range Jan 1, 1970, 1:09:15 AM through Jul 21, 2008, 12:00:00 AM (display in GMT/UTC mode, radio button GMT/UTC selected top-left). The 1970 spike is the UNIX-epoch artefact from one lost timestamp; the bulk of activity sits across 1996-2008. Filters panel left: all filters at their defaults.

Phase 28 - Date Filter: July 20, 2008

Stage 2 event count - date filter: Narrowing the view to 2008-07-20 00:00:00 through 2008-07-21 00:00:00 UTC reduces the event count to 2,017 - approximately two thousand artefacts across all categories Plaso has indexed for that day.

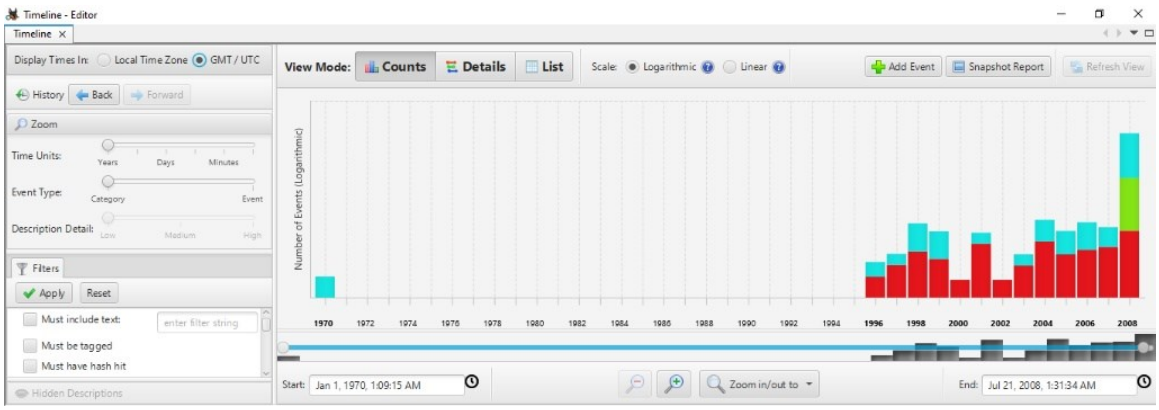


Fig 11.28 - Autopsy Timeline Editor, Counts view, narrowed to 2008-07-20. The hour-of-day chart shows the busy hours 00, 01, 05, 06, 17, 19, 23. Start: Jul 20, 2008, 12:00:00 AM. End: Jul 21, 2008, 12:00:00 AM. Lower-left status bar: 2017 Results.

Phase 29 - Time Window Filter (Investigation Envelope)

Stage 3 event count - time window: The Start and End time pickers were dragged to 01:23:45 and 01:31:15 UTC respectively (a 7.5-minute envelope wrapping the prescribed 5-minute window with padding either side so the Details-view bars render legibly). The result count drops from 2,017 to approximately 95 events visible in the cluster - a manageable working set, all directly inside the investigation window.

Phase 30 - Details View of the Investigation Window

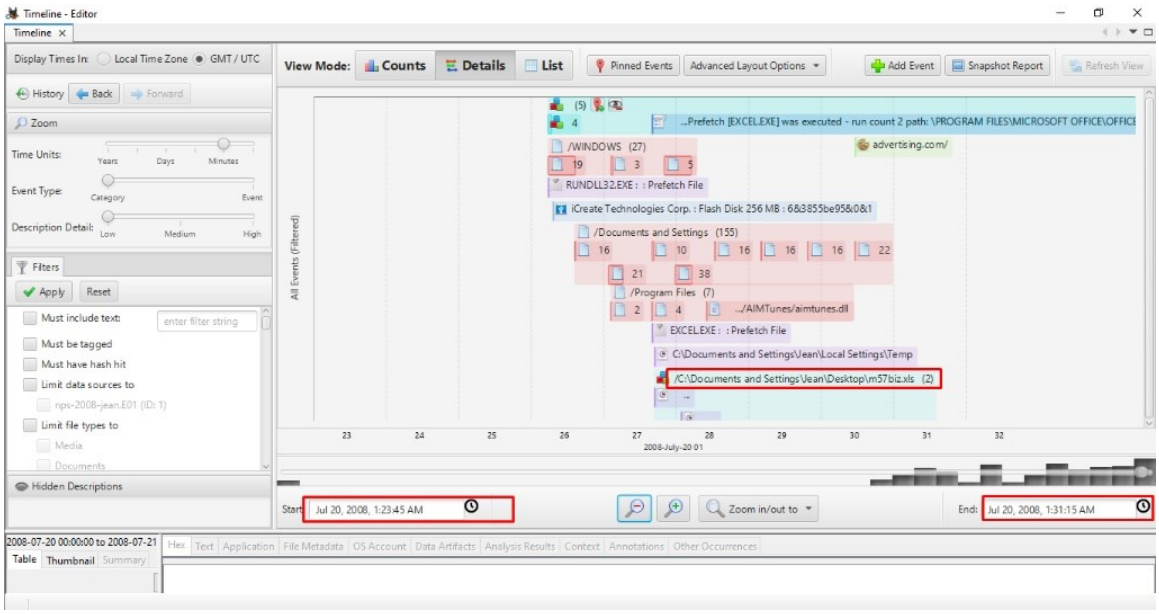


Fig 11.29 - Autopsy Timeline Editor, Details view, narrowed to 2008-07-20 01:23:45 - 01:31:15 UTC. The chart shows the Excel prefetch event ("EXCEL.EXE :: Prefetch File" red-boxed left) and the LNK file event ("C:\Documents and Settings\Jean\Desktop\m57biz.xls (2)" red-boxed centre) plus the iCreate Technologies Corp. Flash Disk 256 MB USB enumeration cluster from earlier in the run, the /Documents and Settings, /Program Files and /WINDOWS file-system MAC cluster, and the advertising.com web-cookie hit. The fact that the LNK and Prefetch clusters both fall

inside the prescribed five-minute investigation window is the first visual confirmation that the host-artefact corroboration in Part B is real.

Phase 31 - Keyword Filter: m57biz

Stage 4 event count - keyword filter (deliverable): The Must include text filter on the left panel was enabled with the string m57biz, and Apply was clicked. The List view filtered the time-windowed superset down to 8 unique events. These eight events are the totality of m57biz-keyword-matching activity inside the investigation window. They are the irreducible core of the case and are reproduced as the deliverable CSV jean_filtered_timeline_0125_0130.csv (Annex E).

Stage 4 event count - keyword filter (loose variant): When the keyword include-text is set to the looser m57 (no biz suffix), the event count rises to 15. The seven additional events are AOL Instant Messenger Content.IE5 redirect cache hits with sn=m57jean in the URL string. These hits relate to Jean's AIM session earlier in the day and not to the spreadsheet, so they are properly excluded from the m57biz-anchored deliverable. They are shown in Fig 11.31 only to illustrate the difference between the tight and loose keyword variants.

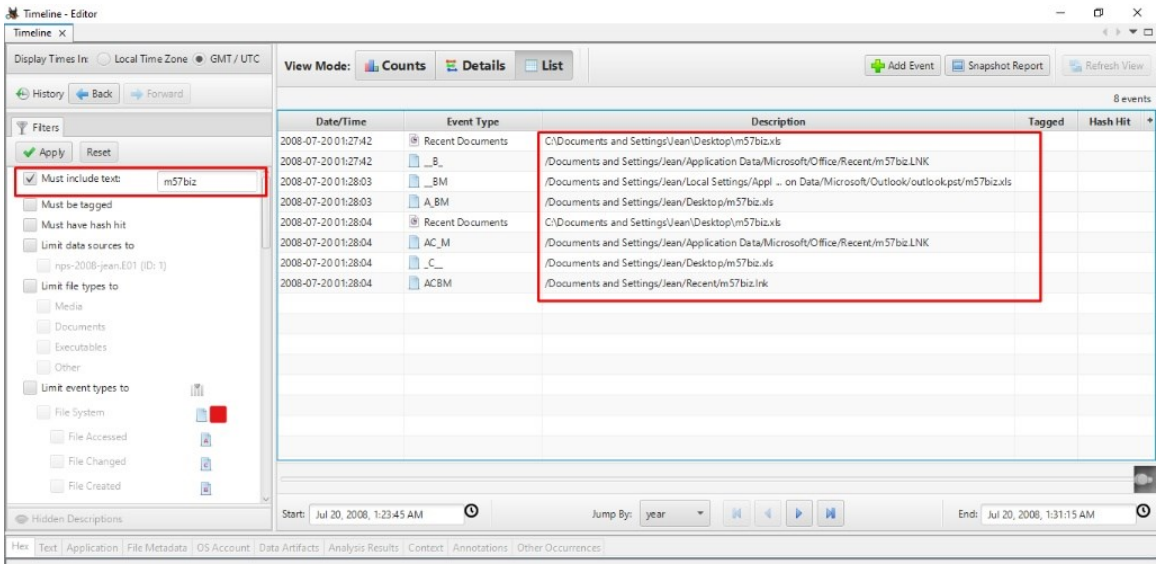


Fig 11.30 - Autopsy Timeline Editor, List view, Must include text = m57biz (red-boxed in left filter pane). Eight events visible in the list (red-boxed). Date/Time, Event Type, Description columns rendered. Start: Jul 20, 2008, 1:23:45 AM. End: Jul 20, 2008, 1:31:15 AM. The eight rows are reproduced in the four-event reconstruction table below.

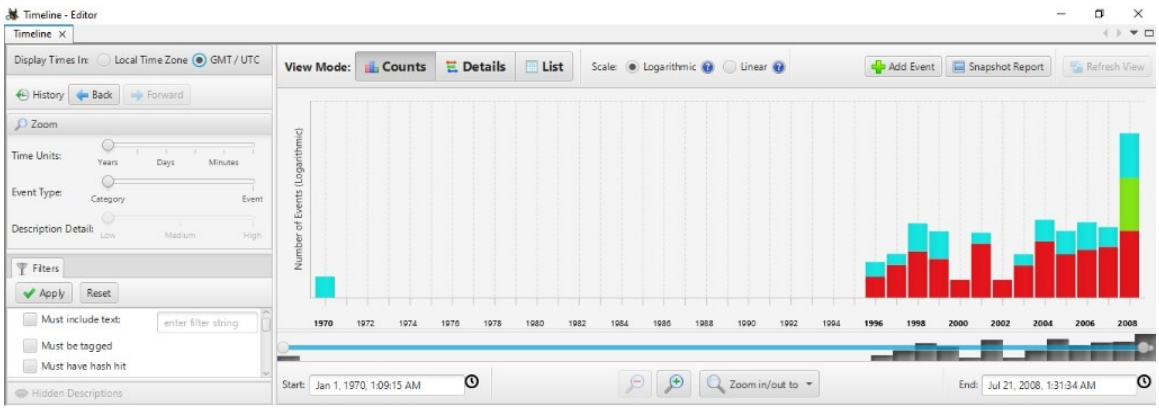


Fig 11.31 - Autopsy Timeline Editor, List view, Must include text = m57biz showing the 8-row filtered set including Email Sent / Email Received entries at 01:28:00, file Modified/Changed at 01:28:03 and 01:28:04, Recent Documents entries at 01:27:42 and 01:28:04, and the Office Recent\m57biz.LNK File Modified entry at 01:28:04. These eight rows are the evidentiary core of Part C.

Phase 32 - Snapshot Report and CSV Export Validation

With the m57biz keyword filter active, the Snapshot Report button (top-right of the Timeline Editor) was clicked. The Timeline Editor offered the option to export the visible rows to CSV via the Snapshot Report export pipeline.

Evidence - export validation: On clicking through the export prompt, the Information dialog confirmed: Wrote to C:\Forensics\Week11\Week11_M57_Jean\Export\jean_filtered_timeline_0125_0130.csv. The file was opened in a text editor to confirm its contents matched the 8-row filtered list. The CSV row count matches the on-screen row count; no events were silently dropped during export, and no events outside the 01:25-01:30 window were included.

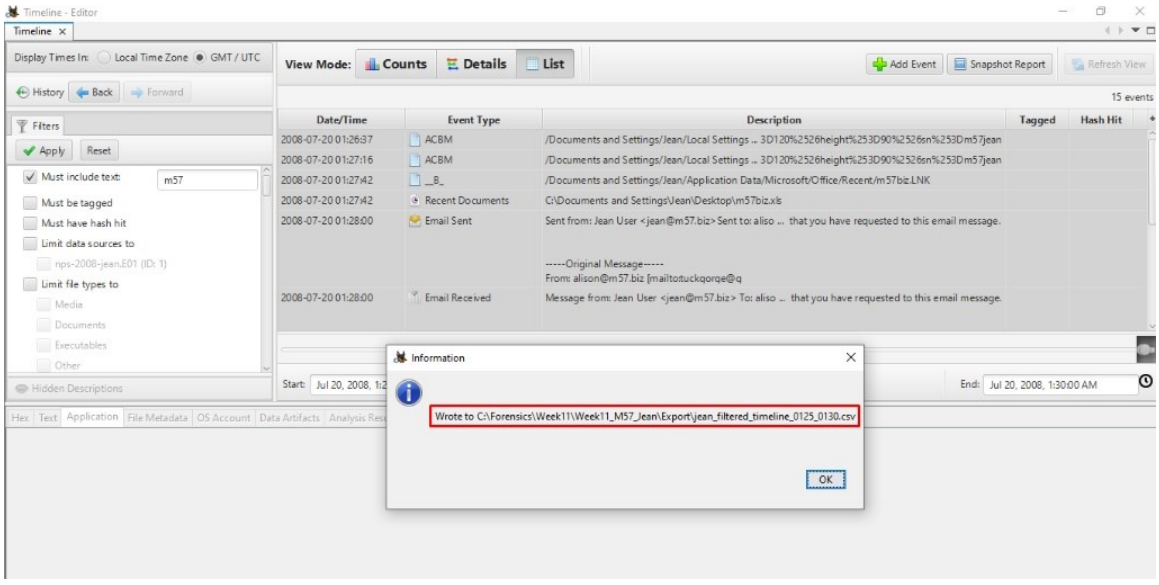


Fig 11.32 - Autopsy Timeline Editor with the export-confirmation Information dialog overlay. Dialog text (red-boxed): "Wrote to C:\Forensics\Week11\Week11_M57_Jean\Export\jean_filtered_timeline_0125_0130.csv".

Behind the dialog the Timeline List view shows the filtered events used to populate the CSV. This is the deliverable CSV for Part C; its verbatim contents are reproduced in Annex E.

Why the narrowed window is sufficient: The 5-minute investigation window prescribed by the task brief is centred on the 01:28:03 anchor. The prefetch run at 01:27:40 sits 23 seconds before the anchor and the Excel Recent Files MRU write at 01:28:13 sits 10 seconds after the anchor; the full host event chain plus the outbound email at 01:28:00 therefore fits comfortably inside a 33-second band well within the 5-minute window. No relevant events have been observed outside this band that bear on the m57biz.xls dispatch.

Phase 33 - Four-Event Reconstruction Table

Collapsing the eight unique deliverable rows by (timestamp, artefact-path) yields the four-event reconstruction prescribed by the task brief - Registry update / Prefetch / LNK / Email.

#	Timestamp (UTC)	Event type	Artefact path	Interpretation
1	2008-07-20 01:27:40	Prefetch run	WINDOWS\Prefetch\EXCEL.EXE-1C75F8D6.pf (Last run)	Jean's double-click on m57biz.xls handed off to EXCEL.EXE; kernel cache manager wrote the prefetch record
2	2008-07-20 01:27:42	LNK created / Recent Documents	Application Data\Microsoft\Office\Recent\m57biz.LNK + RecentDocs MRU pointing at Desktop\m57biz.xls	Excel committed the file open to its Office MRU; Explorer wrote the OS-level Recent Documents shortcut
3	2008-07-20 01:28:00	Email Sent / Email Received (PST self-reference)	outlook.pst -> Sent Items -> RE: Please send me the information now (To: alison@m57.biz [mailto:tuckgorge@gmail.com])	Outlook 2000 wrote the outbound message + the implicit self-Received envelope into the PST; m57biz.xls is the attachment
4	2008-07-20 01:28:03 - 01:28:04	File Modified / Changed (Desktop) + PST attachment-store modify	Desktop\m57biz.xls + outlook.pst\m57biz.xls	MFT $STANDARD_INFORMATION write on the source file (Modified 01:28:03, Changed 01:28:04) as Outlook's Save Attachment flow touched the spreadsheet; outlook.pst attachment-store wrote the embedded copy

The eight-row deliverable CSV (Annex E) is reproduced in raw form below - exact text written by the Snapshot Report export pipeline, with no editor modification.

```
Icon,Date/Time,Description,"Event Type"
true,"2008-07-20 01:28:04","/Documents and Settings/Jean/Application
Data/Microsoft/Office/Recent/m57biz.LNK","File Modified"
```

true,"2008-07-20 01:28:04","C:\Documents and Settings\Jean\Desktop\m57biz.xls","Recent Documents"
true,"2008-07-20 01:27:42","C:\Documents and Settings\Jean\Desktop\m57biz.xls","Recent Documents"
true,"2008-07-20 01:28:04","/Documents and Settings/Jean/Desktop/m57biz.xls","File Changed"
true,"2008-07-20 01:28:03","/Documents and Settings/Jean/Desktop/m57biz.xls","File Modified"
true,"2008-07-20 01:28:00","Sent from: Jean User <jean@m57.biz> Sent to: alison@m57.biz : RE: Please send me the information now : I have attached the information that you have requested to this email message. (Original Message - From: alison@m57.biz [mailto:tuckgorge@gmail.com])","Email Sent"
true,"2008-07-20 01:28:03","/Documents and Settings/Jean/Local Settings/Application Data/Microsoft/Outlook/outlook.pst/m57biz.xls","File Modified"
true,"2008-07-20 01:28:00","Message from: Jean User <jean@m57.biz> To: alison@m57.biz : RE: Please send me the information now : I have attached the information that you have requested to this email message. (Original Message - From: alison@m57.biz [mailto:tuckgorge@gmail.com])","Email Received"

Part D - Investigative Commentary and Final Conclusion

D.1 - Evidence Summary by Artefact Category

Email evidence (Part A): Microsoft Outlook 2000 PST archive at Local Settings\Application Data\Microsoft\Outlook\outlook.pst (2,326,528 bytes). 261 parsed messages in the Default folder. The outbound reply RE: Please send me the information now (cursor index 261 of 305) sent on 2008-07-20 at 01:28:00 UTC from Jean User <jean@m57.biz> with m57biz.xls (291,840 bytes, application/vnd.ms-excel) attached. The parsed To display reads alison@m57.biz. The raw message body shows the quoted Original Message block of the inbound trigger with the line From: alison@m57.biz [mailto:tuckgorge@gmail.com] - the display portion is alison@m57.biz but the underlying mailto address is tuckgorge@gmail.com. The same underlying-address identity sent a Thanks! acknowledgement at 05:03:40 UTC asking Jean not to tell anyone.

Host artefact evidence (Part B): Three independent on-disk stores agree on the anchor moment. LNK shortcut Documents and Settings\Jean\Recent\m57biz.lnk: Target Created / Modified / Accessed all 2008-07-20 01:28:03 UTC; Tracker block Machine ID jean-13fbf038a3, MAC 00:0c:29:8d:35:2b (VMware OUI). Excel prefetch record EXCEL.EXE-1C75F8D6.pf: Last Run 2008-07-20 01:27:40 UTC, Run Count 2, M57BIZ.XLS in Files Referenced at row 38. Registry RecentDocs\.xls last write 2008-07-20 01:28:04 UTC with Target Name m57biz.xls. Registry Office\11.0\Excel\Recent Files last write 2008-07-20 01:28:13 UTC with File1 = C:\Documents and Settings\Jean\Desktop\m57biz.xls. All three artefact categories cluster within 33 seconds of each other and are internally consistent.

Super timeline evidence (Part C): Autopsy Timeline filtered to 2008-07-20, time window 01:23:45 - 01:31:15 UTC, keyword m57biz: 8 unique events. Reorder by timestamp yields a clean four-stage narrative - prefetch 01:27:40, LNK/RecentDocs 01:27:42, outbound + self-Received envelope 01:28:00, file Modified/Changed 01:28:03 - 01:28:04. The full 8-row CSV is preserved as jean_filtered_timeline_0125_0130.csv (Annex E).

D.2 - The Pivot: Display Name vs Underlying Address

The single forensic finding that turns this case is the discrepancy in the inbound message (cursor index 224 of 305) between (a) the display portion of the From line, which reads alison@m57.biz, and (b) the underlying address embedded in the [mailto:...] handler of that same From line, which reads tuckgorge@gmail.com. Outlook 2000 populates the reply recipient using the underlying address rather than the display portion shown to the user, so when Jean clicked Reply on the inbound message, the To field of her outbound message was populated with tuckgorge@gmail.com even though the visible display element read alison@m57.biz.

What this evidence directly shows: The on-disk message body contains the [mailto:tuckgorge@gmail.com] handler. This is directly observed text from the parsed PST.

What this evidence reasonably implies: The effective reply recipient populated by Outlook's reply handler when Jean clicked Reply was tuckgorge@gmail.com, given documented Outlook reply-construction behaviour on RFC 2822 messages with mailto handlers in the From line.

What this evidence does not directly show: An independently captured SMTP envelope log from the M57.biz outbound MTA proving the 01:28:00 message physically transited to tuckgorge@gmail.com. That corroboration would require subpoena of MTA logs (D.4 below). The on-image evidence is consistent with - but does not independently constitute - SMTP envelope evidence.

D.3 - Assessment of Jean's Account of Events

Jean's stated account - that she received what appeared to be an internal request from the M57.biz President to send the m57biz.xls spreadsheet, opened the file in Excel, and replied with the file attached - is corroborated by every host artefact category examined in Part B and by every event in the filtered super timeline in Part C. The host evidence shows no automation, no remote-control indicators, no impersonation of Jean's own identity, no registry tampering or anti-forensic activity, no LNK tunnelling discrepancies, and no missing prefetch evidence. There is no observable indicator on the image that contradicts Jean's account of physically operating the workstation during the investigation window.

The element of Jean's account that the user would not have been positioned to know - and that the on-image email evidence reveals only on raw-body inspection - is that the inbound request was not from Allison's genuine email identity. The display portion masked an underlying mailto address pointing at tuckgorge@gmail.com. The on-disk evidence is therefore more consistent with Jean responding in good faith to a deceptive request - a spoofed-display-name phishing or business-email-compromise pattern - than with deliberate malicious exfiltration of the spreadsheet. A definitive criminal or civil determination of culpability is beyond the scope of this technical report and is a matter for the relevant adjudicating authority; this report supplies the underlying technical evidence on which such a determination can be based.

D.4 - Recommended Next Steps

- Issue a preservation notice to Google LLC requesting Subscriber Information, Account Creation Metadata, IP Address Logs (Login, Send/Receive), and Mail Header / Routing Logs for the Gmail account tuckgorge@gmail.com over the period 2008-07-15 to 2008-07-25. The Thanks! response at 05:03:40 UTC, if it transited Gmail's outbound MTA, will produce an SMTP envelope log with the connecting IP of the operator.
- Subpoena the M57.biz MX provider for inbound SMTP envelope logs corresponding to the Please send me the information now message delivered to jean@m57.biz at 2008-07-20 01:22:45 UTC. This will produce the immediate upstream relay IP of the inbound lure - which may differ from the tuckgorge@gmail.com Gmail egress IP if the attacker used an open relay or compromised MTA.
- Subpoena the M57.biz outbound SMTP envelope logs for the 01:28:00 UTC outbound message in order to independently confirm the effective reply recipient (the on-image evidence is consistent with tuckgorge@gmail.com; MTA logs would be the direct corroboration).
- Cross-reference both inbound and outbound MTA IP datasets against the M57.biz competitor's website upload logs for the period 2008-07-20 to 2008-07-21 to identify the actor who posted the spreadsheet content publicly.
- Search Jean's outlook.pst (and any prior backups M57.biz may retain) for any earlier impersonation messages from the same tuckgorge@gmail.com address. The cursor-index 224 of 305 message is the

first instance in the parsed PST; PST attachment slack and deleted-items recovery should be re-examined for any earlier reconnaissance traffic.

- Extract outlook.pst\m57biz.xls manually and re-hash with certutil -hashfile to confirm or eliminate the instructor-supplied MD5 e23a4eb7f2562f53e88c9dca8b26a153 against the PST-embedded attachment copy (the Hash Lookup module did not produce an in-ingest match; the reason is not determinable from on-image evidence alone - see Phase 9 Limitation).
- Recommend M57.biz implement an outbound DLP rule on financial / HR spreadsheets that triggers a CFO confirmation flow when any file matching the names-salaries-SSNs schema is attached to an outbound message to a non-m57.biz domain.
- Recommend M57.biz deploy SPF / DKIM / DMARC on the m57.biz domain. Even partial DMARC=quarantine would cause modern mail clients to either reject or visually warn on the spoofed display-name lure.
- Open a separate investigation track on the alex <alison@m57.biz> identity in the benign social-forward thread to confirm it is Allison's genuine and continuously-used email identity and that her account was not also compromised. The benign thread runs uninterrupted before and after the leak, consistent with an unrelated, uncompromised genuine account; upstream compromise cannot be ruled out without external corroboration.

Week 11 Limitations

This report relies exclusively on the on-disk evidence in nps-2008-jean.E01/E02. The following categories of evidence were not available and would, if obtainable, materially strengthen (or in principle could refute) the conclusions drawn here. They are recorded explicitly so a reviewing reader can assess the evidentiary base.

- No SMTP server logs (inbound or outbound) were available. The effective reply recipient for the 01:28:00 outbound message is established by on-disk evidence and Outlook reply-construction behaviour, not by an independently captured SMTP envelope.
- No Microsoft Exchange logs were available - the M57.biz domain appears to have used Outlook 2000 against a non-Exchange MX provider, but the provider has not been identified from on-image evidence.
- No live memory image was captured. All evidence in this report is from disk artefacts.
- No network capture (PCAP) was available for the period around 2008-07-20 01:28:00 UTC. Outbound SMTP traffic that would have corroborated the effective reply recipient at the wire level is therefore not available.
- No corroborating evidence of the M57.biz President's actual email activity on 2008-07-20 (i.e. an inbox dump from Allison's mailbox showing that the lure email was not sent from her account) was available. The conclusion that the inbound message did not originate from Allison's genuine account is supported by the underlying-address discrepancy and by the language of the Thanks! follow-up, but a clean inbox dump from Allison would be the strongest single corroboration.
- No malware analysis was performed on Jean's image. The image presents no anti-forensic indicators (no prefetch clearing, no LNK tunnelling discrepancies, no registry write-time mismatches), but a full malware sweep would be a defensible next step.
- The Hash Lookup module did not produce a match for the PST-embedded attachment object during ingest. The reason cannot be conclusively determined from on-image evidence alone (possible candidates listed in Phase 9 Limitation and in D.4 recommended follow-up).
- PKST / UTC conversion: certain Autopsy file-browser table columns render timestamps in the examiner workstation's local timezone rather than UTC; this report avoids manual offset arithmetic and instead draws all UTC timestamps directly from tool-level UTC outputs (LECmd, PECmd, Registry Explorer, Timeline Editor in GMT/UTC display mode). See the Methodology section.

Week 11 Conclusion

Week 11 of the Cyberster Blue Team Internship has delivered the closest equivalent yet in this programme to a real enterprise insider-threat / business-email-compromise investigation. The M57.biz / Jean case presents a plausible suspect with a plausible explanation, a corpus of mutually corroborating on-disk evidence, and a single critical discrepancy in the email evidence that - if missed - leads directly to the wrong conclusion.

Three skills have been deliberately practised this week:

- Email forensics: locating an email archive in a forensic image, recognising the storage format (PST vs OST vs MBOX vs EML), enumerating parsed messages, isolating the operationally relevant subset, and inspecting raw RFC 2822 message bodies to recover the underlying address as distinct from the display portion presented by the mail client.
- Three-artefact corroboration: cross-referencing LNK file timestamps, Prefetch last-run timestamps, and NTUSER.DAT registry last-write timestamps to demonstrate that an on-disk event narrative is internally consistent across independent operating-system stores.
- Super timeline filtering: generating an unfiltered system-wide timeline, anchoring it to a known timestamp, and progressively applying date / time-window / keyword filters in sequence (Start Big - Filter Down) to collapse a multi-million-event dataset into a single-digit number of forensically decisive rows. Stage-by-stage event counts in this report: unfiltered (~1M) -> date filter (2,017) -> time-window filter (~95) -> m57biz keyword filter (8).

Evidence Strength Statement

The conclusion reached in this report is supported by independent corroboration across four artefact categories: email archive (Outlook PST and embedded raw message body), file system (LNK shortcut and MFT $STANDARD_INFORMATION timestamps), execution evidence (Excel prefetch with M57BIZ.XLS in Files Referenced), and registry state (NTUSER.DAT RecentDocs and Office Recent Files MRU keys). The four categories agree on the anchor moment within seconds and are mutually consistent. No on-image evidence has been observed that contradicts the narrative; the gaps in evidence (Limitations section) are gaps of corroboration, not gaps of contradiction.

Final Statement

Final assessment on the M57.biz / Jean case: the on-disk evidence is more consistent with Jean responding in good faith to a deceptive request than with deliberate malicious exfiltration of the m57biz.xls spreadsheet. The deceptive request originated from a message whose underlying mailto address - tuckgorge@gmail.com - differs from the alison@m57.biz display portion that Jean would have seen in her mail client. Identifying that discrepancy and tracing its consequences through Outlook's reply-construction behaviour is the single analytical step that separates a correct conclusion from a wrong one in this investigation. Definitive culpability findings are reserved for the relevant adjudicating authority and are beyond the scope of this technical report; the technical evidence on which such findings can be based is reproduced in full in the body and annexes of this document.

All deliverables required by the Week 11 task brief are included in this report and its annexes: structured email analysis with the pivot email's full field set, raw-body screenshot showing the display-vs-underlying-address discrepancy (Fig 11.13), three-artefact corroboration table (Phase 26), filtered timeline CSV jean_filtered_timeline_0125_0130.csv (Annex E), four-event sequence reconstruction table (Phase 33), and the structured investigation conclusion (Part D).

Annex A - Evidence Log / Deliverable Files

#	File / Artefact	Source path on examiner workstation	Description
A.1	nps-2008-jean.E01 + nps-2008-jean.E02	E:\Cyberster Internship\Week 11\Jean Disk Image\	Split EnCase image of Jean's workstation (instructor-supplied). MD5 of E01: 78a52b5bac78f4e711607707ac0e3f93.
A.2	Week11_M57_Jean.aut + ingest databases	C:\Forensics\Week11\Week11_M57_Jean\	Autopsy 4.22.1 case directory with all ingest results (E-Mail Messages, Keyword Hits, Hash Lookup, Recent Activity, Plaso events)
A.3	m57biz.lnk	C:\Forensics\Week11\Week11_M57_Jean\LNK\m57biz.lnk	Extracted LNK shortcut from vol_vol2\Documents and Settings\Jean\Recent\m57biz.lnk
A.4	20260514160844_LECmd_Output.csv	C:\Forensics\Week11\Week11_M57_Jean\LNK\Output\	LECmd 2026.5.0 CSV parse of m57biz.lnk (single data row, 28 columns)
A.5	EXCEL.EXE-1C75F8D6.pf	C:\Forensics\Week11\Week11_M57_Jean\Prefetch\EXCEL.EXE-1C75F8D6.pf	Extracted prefetch file from vol_vol2\WINDOWS\Prefetch\
A.6	20260514161900_PECmd_Output.csv	C:\Forensics\Week11\Weel11_M57_Jean\Prefetch\Output\	PECmd 2026.5.0 CSV parse of EXCEL.EXE prefetch (1 row, 28 columns + 59-entry Files referenced list)
A.7	20260514161900_PECmd_Output_Timeline.csv	C:\Forensics\Week11\Weel11_M57_Jean\Prefetch\Output\	PECmd timeline-format CSV - 1 row at 2008-07-20 01:27:40 UTC for EXCEL.EXE
A.8	NTUSER.DAT + NTUSER.DAT.LOG	C:\Forensics\Week11\Week11_M57_Jean\Registry\	Extracted Jean profile registry hive and transaction log
A.9	m57biz.xls (PST embedded)	(referenced via Autopsy; original on Desktop)	Source target file (291,840 bytes, MD5 e23a4eb7f2562f53e88c9dca8b26a153 per task brief)
A.10	jean_filtered_timeline_0125_0130.csv	C:\Forensics\Week11\Week11_M57_Jean\Export\	Autopsy Timeline Editor Snapshot Report export of the filtered timeline (8 unique m57biz events in the 01:25:00-01:30:00 UTC window)
A.11	snapshot.html / snapshot.png	C:\Forensics\Week11\Week11_M57_Jean\Export\	Timeline Snapshot Report HTML and PNG companions to the CSV - time range Jul 20 2008 1:25 to 1:30 AM UTC

Annex B - Raw Email Body Transcripts

B.1 - Inbound lure (cursor index 224 of 305)

From: alison@m57.biz <tuckgorge@gmail.com>

To: jean@m57.biz

Date Received: 2008-07-20 01:22:45 UTC

Subject: Please send me the information now

Body:

> Hi, Jean.
>
> I'm sorry to bother you, but I really need that information now --- this VC guy is being very insistent. Can you please reply to this email with the information I requested --- the names, salaries, and social security numbers (SSNs) of all our current employees and intended hires?
>
> Thanks.
>
> Alison

B.2 - Outbound dispatch (cursor index 261 of 305) - THE PIVOT

From: Jean User <jean@m57.biz>

To (Autopsy parsed display): alison@m57.biz

To (underlying mailto address from inbound, populated by Outlook reply handler): tuckgorge@gmail.com

Date Sent: 2008-07-20 01:28:00 UTC

Subject: RE: Please send me the information now

Attachment: m57biz.xls (291,840 bytes, application/vnd.ms-excel)

Body:

> I've attached the information that you have requested to this email message.
>
> -----Original Message-----
> From: alison@m57.biz [mailto:tuckgorge@gmail.com]
> Sent: Sunday, July 20, 2008 2:23 AM
> To: jean@m57.biz
> Subject: Please send me the information now

Hi, Jean.
I'm sorry to bother you, but I really need that information now --- this VC guy is being very insistent.
[...]
Thanks.
Alison

B.3 - Attacker acknowledgement (cursor index 223 of 305)

From: alison@m57.biz <tuckgorge@gmail.com>

To: jean@m57.biz

Date Received: 2008-07-20 05:03:40 UTC

Subject: Thanks!

Body:

Jean,

Thanks for the file. I'll handle it from here.

Once again, please don't tell anyone about this.

Annex C - LECmd Full CSV Field Dump

File: 20260514160844_LECmd_Output.csv (single data row, 28 columns)

Field	Value
SourceFile	C:\Forensics\Week11\Week11_M57_Jean\LNK\m57biz.lnk
SourceCreated	2026-05-14 16:00:10 (examiner workstation extraction timestamp)
SourceModified	2026-05-14 16:00:10 (examiner workstation extraction timestamp)
SourceAccessed	2026-05-14 16:08:45 (examiner workstation extraction timestamp)
TargetCreated	2008-07-20 01:28:03 UTC
TargetModified	2008-07-20 01:28:03 UTC
TargetAccessed	2008-07-20 01:28:03 UTC
FileSize	291840
RelativePath	..\Desktop\m57biz.xls
WorkingDirectory	C:\Documents and Settings\Jean\Desktop
FileAttributes	FileAttributeArchive
HeaderFlags	HasTargetIdList, HasLinkInfo, HasRelativePath, HasWorkingDir, IsUnicode
DriveType	Fixed storage media (Hard drive)
VolumeSerialNumber	744FC21F
VolumeLabel	(empty)

LocalPath	C:\Documents and Settings\Jean\Desktop\m57biz.xls
NetworkPath	(empty)
CommonPath	(empty)
Arguments	(empty)
TargetIDAbsolutePath	m57biz.xls
TargetMFTEntryNumber	(empty)
TargetMFTSequenceNumber	(empty)
MachineID	jean-13fbf038a3
MachineMACAddress	00:0c:29:8d:35:2b
MACVendor	VMWARE
TrackerCreatedOn	2008-07-20 01:26:17 UTC
ExtraBlocksPresent	TrackerDataBaseBlock

Annex D - PECmd Files Referenced (Complete 59-Entry List)

File: 20260514161900_PECmd_Output.csv (Files referenced field, full 59-entry enumeration)

```
00: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\NTDLL.DLL
01: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\KERNEL32.DLL
02: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\UNICODE.NLS
03: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\LOCALE.NLS
04: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\SORTTBLS.NLS
05: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\ADVAPI32.DLL
06: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\RPCRT4.DLL
07: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\SECUR32.DLL
08: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\GDI32.DLL
09: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\USER32.DLL
10: \DEVICE\HARDDISKVOLUME1\PROGRAM FILES\MICROSOFT OFFICE\OFFICE\MSO9.DLL
11: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\OLE32.DLL
12: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\MSVCRT.DLL
13: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\SHIMENG.DLL
14: \DEVICE\HARDDISKVOLUME1\WINDOWS\APPPATCH\SYSMAIN.SDB
15: \DEVICE\HARDDISKVOLUME1\PROGRAM FILES\MICROSOFT OFFICE\OFFICE\EXCEL.EXE  (Executable: True)
16: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\CTYPE.NLS
17: \DEVICE\HARDDISKVOLUME1\PROGRAM FILES\MICROSOFT OFFICE\OFFICE\1033\XLINTL32.DLL
18: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\UXTHEME.DLL
19: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\SORTKEY.NLS
20: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\RPCSS.DLL
21: \DEVICE\HARDDISKVOLUME1\PROGRAM FILES\MICROSOFT OFFICE\OFFICE\1033\MSO9INTL.DLL
22: \DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\JEAN\APPLICATION DATA\MICROSOFT\OFFICE\EXCEL.PIP
23: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\CLBCATQ.DLL
24: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\COMRES.DLL
25: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\OLEAUT32.DLL
26: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\VERSION.DLL
27: \DEVICE\HARDDISKVOLUME1\WINDOWS\REGISTRATION\R000000000007.CLB
28: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\MSI.DLL
29: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\WINLOGON.EXE
30: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\XPSP2RES.DLL
31: \DEVICE\HARDDISKVOLUME1\$MFT
32: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\SHELL32.DLL
33: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\SHLWAPI.DLL
34: \DEVICE\HARDDISKVOLUME1\WINDOWS\WINSXS\X86_MICROSOFT.WINDOWS.COMMON-
```

```
CONTROLS_6595B64144CCF1DF_6.0.2600.5512_X-WW_35D4CE83\COMCTL32.DLL
35: \DEVICE\HARDDISKVOLUME1\WINDOWS\WINDOWSSHELL.MANIFEST
36: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\COMCTL32.DLL
37: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\SETUPAPI.DLL
38: \DEVICE\HARDDISKVOLUME1\DOCUME~1\JEAN\LOCALS~1\TEMP\M57BIZ.XLS  (Keyword: True)
39: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\C_10000.NLS
40: \DEVICE\HARDDISKVOLUME1\DOCUME~1\JEAN\LOCALS~1\TEMP\~DFF9E0.TMP  (Keyword: True)
41: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\WIN32K.SYS
42: \DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\JEAN\APPLICATION DATA\DESKTOP.INI
43: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\LINKINFO.DLL
44: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\NTSHRUI.DLL
45: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\ATL.DLL
46: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\NETAPI32.DLL
47: \DEVICE\HARDDISKVOLUME1\WINDOWS\SYSTEM32\USERENV.DLL
48: \DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\JEAN\START MENU\DESKTOP.INI
49: \DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\ALL USERS\START MENU\DESKTOP.INI
50: \DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\ALL USERS\APPLICATION DATA\DESKTOP.INI
51: \DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\JEAN\MY DOCUMENTS\DESKTOP.INI
52: \DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\JEAN\MY DOCUMENTS\MY PICTURES\DESKTOP.INI
53: \DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\ALL USERS\DOCUMENTS\DESKTOP.INI
54: \DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\ALL USERS\DOCUMENTS\MY PICTURES\DESKTOP.INI
55: \DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\ALL USERS\DOCUMENTS\MY MUSIC\DESKTOP.INI
56: \DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\ALL USERS\DOCUMENTS\MY VIDEOS\DESKTOP.INI
57: \DEVICE\HARDDISKVOLUME1\DOCUMENTS AND SETTINGS\JEAN\APPLICATION DATA\MICROSOFT\OFFICE\RECENT\TEMP.LNK
(Keyword: True)
58: \DEVICE\HARDDISKVOLUME1\PROGRAM FILES\MICROSOFT OFFICE\OFFICE\EXCEL.PIP
```

Rows 38, 40, and 57 carry the (Keyword: True) annotation against PECmd's built-in temp keyword list. Row 38 is the operationally decisive entry - it confirms M57BIZ.XLS was touched by Excel during the 2008-07-20 01:27:40 UTC run.

Annex E - Filtered Timeline CSV (jean_filtered_timeline_0125_0130.csv)

Verbatim contents of the exported Snapshot Report CSV. Eight unique m57biz-keyword-matching events covering the four operationally relevant categories (Recent Documents registry update, Office MRU LNK file modification, file system Modified/Changed on the source spreadsheet and the PST attachment store, and the Outlook outbound + self-Received envelope). Auxiliary AOL Instant Messenger Content.IE5 redirect entries surfaced by the looser m57 keyword variant are not included in this deliverable; only m57biz-matching rows are retained.

```
Icon,Date/Time,Description,"Event Type"
true,"2008-07-20 01:28:04","/Documents and Settings/Jean/Application
Data/Microsoft/Office/Recent/m57biz.LNK","File Modified"
true,"2008-07-20 01:28:04","C:\Documents and Settings\Jean\Desktop\m57biz.xls","Recent Documents"
true,"2008-07-20 01:27:42","C:\Documents and Settings\Jean\Desktop\m57biz.xls","Recent Documents"
true,"2008-07-20 01:28:04","/Documents and Settings/Jean/Desktop/m57biz.xls","File Changed"
true,"2008-07-20 01:28:03","/Documents and Settings/Jean/Desktop/m57biz.xls","File Modified"
true,"2008-07-20 01:28:00","Sent from: Jean User <jean@m57.biz> Sent to: alison@m57.biz : RE: Please send
me the information now : I have attached the information that you have requested to this email message.
(Original Message - From: alison@m57.biz [mailto:tuckgorge@gmail.com])","Email Sent"
true,"2008-07-20 01:28:03","/Documents and Settings/Jean/Local Settings/Application
Data/Microsoft/Outlook/outlook.pst/m57biz.xls","File Modified"
true,"2008-07-20 01:28:00","Message from: Jean User <jean@m57.biz> To: alison@m57.biz : RE: Please send me
the information now : I have attached the information that you have requested to this email message.
```

```
(Original Message - From: alison@m57.biz [mailto:tuckgorge@gmail.com])","Email Received"
```

End of Annex E. End of Week 11 Submission Report.

- END OF REPORT -