DIGITAL FORENSIC EXAMINATION REPORT

Windows Registry Artifact Analysis

The State vs. Wes Mantooth, Digital Media Examination

MULTI-SOURCE EXAMINATION · AUTOPSY · REGRIPPER · HOST BASELINE

REPORT ID	DFCS · CCFA · MANTOOTH · 2026-07
PREPARED BY	Awais Ahmed
ACADEMIC PROGRAM	B.S. Digital Forensics and Cyber Security (DFCS)
CERTIFICATION TRACK	Certified Computer Forensics Analyst (CCFA)
EVIDENCE REFERENCE	Mantooth.E01: Forensic Disk Image (Partition 1, MANTOOTH [NTFS])
EXAMINATION FOCUS	Windows Registry Hives: SAM, SECURITY, SOFTWARE, SYSTEM, NTUSER.DAT
PRIMARY TOOLS	Autopsy 4.23.1 · RegRipper 3.0 (master) · AccessData FTK Imager · Registry Editor
REPORT DATE	July 20, 2026
CLASSIFICATION	Academic Coursework: Portfolio Release Copy

This document reproduces coursework performed against a training forensic image ("Mantooth") used for digital forensics education. All findings were independently derived and cross-validated across three examination sources by the author.

Report Details

Field	Detail
EXAMINER	Awais Ahmed
ROLE	Digital Forensics Student / Examiner-in-Training
SOURCE PRACTICALS	"Week 1: Windows Registry Practical" and "System Forensic" worksheets
EVIDENCE CUSTODIAN	Course-provided image (Mantooth.E01), examined in a controlled lab environment

Table of Contents

Report Details 2
Table of Contents 2
1. Executive Summary 4
2. Case Background 4
3. Methodology 4
3.1 Examination Environment and Tools 4
3.2 Three-Source Examination Approach 5
3.3 Registry Hive Locations 5
3.4 Report Structure 5
4. Findings 5
Finding 1, Computer Name 6
Finding 2, System Time Zone 7
Finding 3, IDE Hard Drive Enumeration 9
Finding 4, Configured IP Address / DHCP Information 11
Finding 5, Prefetch Parameters (EnablePrefetcher) Setting 12
Finding 6, TrueCrypt Service Start Type 14
Finding 7, Last Recorded System Shutdown Time 15
Finding 8, Canon PowerShot SD500: Device Serial / Connection Time 17
Finding 9, Five Portable Devices Connected to the System 18
Finding 10, Default Web Browser 20
Finding 11, Network Interface Cards Installed 21
Finding 12, Configured Wireless Network Profile Name 22
Finding 13, Three Removable Storage Devices (Last-Write, Serial, Drive Letter) 26
Finding 14, Five Installed Software Titles (with Install Timestamps) 28
Finding 15, Registered Organization, Install Date, Product ID, Product Name, Registered Owner 34
Finding 16, User Profiles Present on the System 35

Finding 17, SAM Account Details Per User (Login Count, Last Login, Failed Logins) 37
Finding 18, Which User Account Warrants Further Investigation, and Why 42
Finding 19, Recent PDF Files Opened by Wes Mantooth 42
Finding 20, Three Most Recent Paint Files 44
Finding 21, Five Most Recently Used Run Commands 45
Finding 22, File Path for ATM_THEFTS1.ppt 47
Finding 23, Recommended Investigator Response to Finding 22 48
Finding 24, Internet Explorer Start Page 48
Finding 25, Internet Explorer Default Download Directory 49
Finding 26, Internet Explorer Address-Bar / Favorites Activity 49
Finding 27, Media Player Files Referenced from the F: Drive 50
Finding 28, Recommended Investigator Response to Finding 27 51
Finding 29, Two Most Recent PowerPoint Files 51
Finding 30, Five Items in the Recent Documents List and Their Investigative Value 51
1. Vista Mantooth Bitlocker Key 1.4.txt 52
2. CC Nums.xls 52
3. ATM_THEFTS1.ppt 52
4. BestCrypt Prefetch/Uninstall Evidence 52
5. securityevt.evtx / testevt.evtx / Internet Explorer.evtx 52
Finding 31, Five Programs Listed in the Run/RunMRU Key 55
Finding 32, Five URLs Typed into Internet Explorer 56
Finding 33, Email Addresses / Usernames Associated with Mantooth 58
Finding 34, WinVNC Remote Access Password 59
Finding 35, Yahoo Messenger Username 60
Finding 36, Default Printer Details 61
5. Case Assessment and Investigative Conclusions 61
5.1 Account Activity 62
5.2 Financial-Crime Indicators 62
5.3 Anti-Forensic / Concealment Indicators 62
5.4 Recommended Next Steps 62
5.5 Methodology Note 62
Appendix A, Registry Hive and Key Reference 62
Appendix B, Tools and Versions 63

1. Executive Summary

This report documents a Windows Registry forensic examination performed against the “Mantooth” training disk image (Mantooth.E01) as part of Digital Forensics and Cyber Security (DFCS) coursework aligned to Certified Computer Forensics Analyst (CCFA) competencies. The objective was to reconstruct system configuration, user activity, and connected-device history for a single user account of interest, Wes Mantooth, entirely from registry artifacts.

Thirty-six examination questions were answered. For every question, the finding was independently derived from up to three sources and cross-checked for consistency:

- Autopsy, the case-loaded Mantooth.E01 image, examined through its built-in Registry and Recent Activity modules.
- RegRipper-parsed hive output, the SAM, SECURITY, SOFTWARE, SYSTEM and NTUSER.DAT hives were extracted from the image via FTK Imager and parsed offline into plugin-based .txt reports using RegRipper 3.0.
- Host baseline comparison, the same artifact categories were pulled from the examiner's own live Windows registry (HP laptop) to illustrate how each key behaves on a known, non-evidentiary system.

Cross-source validation surfaced several evidentiary items of investigative significance, most notably: a BitLocker recovery key file, a spreadsheet named consistent with stored credit card numbers, a presentation titled ATM_THEFTS1.ppt, Prefetch evidence that the disk-encryption utility BestCrypt was executed, a plaintext-recoverable WinVNC remote-access password, and login/failed-login timestamps for two user accounts (Wes Mantooth and Dracula) that failed within one second of each other. These findings, and their recommended investigative follow-up, are detailed in Sections 4 and 5.

2. Case Background

The Mantooth scenario is a widely used digital forensics training image built around a fictional financial-crime investigation. The disk image (Mantooth.E01) represents a single-partition NTFS system (volume label MANTOOTH) seized as evidence, containing multiple local user profiles including Wes Mantooth, Dracula, and other named accounts.

The investigative premise treats Wes Mantooth as the primary subject of interest. Filenames and artifacts recovered from his profile, including references to ATM-related theft material, a file suggestive of stored credit card numbers, and encryption/anti-forensic tool usage, point toward a financial-crime narrative involving unauthorized access to card data and possible concealment of evidence through disk or file encryption.

This report treats the image strictly as coursework evidence: all conclusions are drawn only from what the registry artifacts themselves support, and every finding is framed the way it would be in a real examination, as an artifact with a source, a path, and an evidentiary interpretation, not as a proven fact about a real person or event.

3. Methodology

3.1 Examination Environment and Tools

The examination was carried out in a controlled lab environment using the following tools:

- Autopsy 4.23.1, used to mount and browse the Mantooth.E01 image, and to inspect registry and recent-activity artifacts directly within the case.

- AccessData FTK Imager, used to navigate the image's file system and export the raw registry hive files for offline parsing.
- RegRipper 3.0 (master branch, github.com/keydet89/RegRipper3.0), used to run hive-specific plugins against each exported hive and generate structured, human-readable .txt reports.
- Windows Registry Editor (regedit) on the examiner's own HP laptop, used as a live, known-good baseline for comparison against the evidentiary artifacts.

3.2 Three-Source Examination Approach

Each of the 36 questions below was answered three times, from three independent vantage points, rather than relying on a single tool's output. This mirrors real-world practice, where a single-source finding is treated as provisional until corroborated:

- Source 1: Autopsy: the interpreted, GUI-level view of the artifact as Autopsy's registry parser presents it inside the loaded case.
- Source 2: RegRipper Parsed Hive Output: the same artifact re-derived independently from the raw exported hive, using purpose-built RegRipper plugins, to confirm Autopsy's interpretation against the underlying registry data.
- Source 3: Host Registry Comparison: the equivalent key pulled from a live, non-evidentiary Windows installation, to establish what the artifact normally looks like absent any suspicious modification, and to sanity-check the examiner's own tooling and technique.

Where an artifact is inherently specific to the Mantooth image (a particular file path, an MRU entry, a stored credential), no equivalent exists on the comparison host; this is marked “Not applicable” rather than omitted, so the absence of a third source is explicit rather than silent.

3.3 Registry Hive Locations

The following hives were located and extracted from the Mantooth image via FTK Imager prior to RegRipper analysis:

```
Mantooth.E01 / Partition 1 / MANTOOTH [NTFS] / [root] / Windows / System32 / config /
```

- SAM
- SECURITY
- SOFTWARE
- SYSTEM

Two per-user NTUSER.DAT hives were additionally extracted to examine user-specific activity:

```
Mantooth.E01 / Partition 1 / MANTOOTH [NTFS] / [root] / Users / Wes Mantooth /
NTUSER.DAT

Mantooth.E01 / Partition 1 / MANTOOTH [NTFS] / [root] / Users / Dracula / NTUSER.DAT
```

SYSTEM and SOFTWARE hive plugins were used to answer questions 1–16; the SAM hive was used for question 17–18 (user account auditing); and Wes Mantooth's NTUSER.DAT was used for questions 19–36 (user-level activity, MRU lists, and application-specific credentials).

3.4 Report Structure

Section 4 presents all 36 findings in the order examined. Each finding states the question, the three-source evidence, and, for items of direct investigative significance, a short forensic-significance note explaining why the artifact matters and what it would justify doing next. Section 5 consolidates the case-critical findings into an overall assessment.

4. Findings

Findings are numbered to match the original practical worksheet (Questions 1–36). Each finding is labeled by source rather than by letter, to keep attribution unambiguous.

Finding 1, Computer Name

Purpose: Establishes the system's assigned hostname, used to positively identify this machine across every other artifact in the examination.

Source 1: Autopsy

Registry path: `SYSTEM\ControlSet001\Control\ComputerName\ComputerName`

Result: ComputerName = WESMANTOOTH-PC (Owner: Wes Mantooth; Organization: Volturi Enterprises).

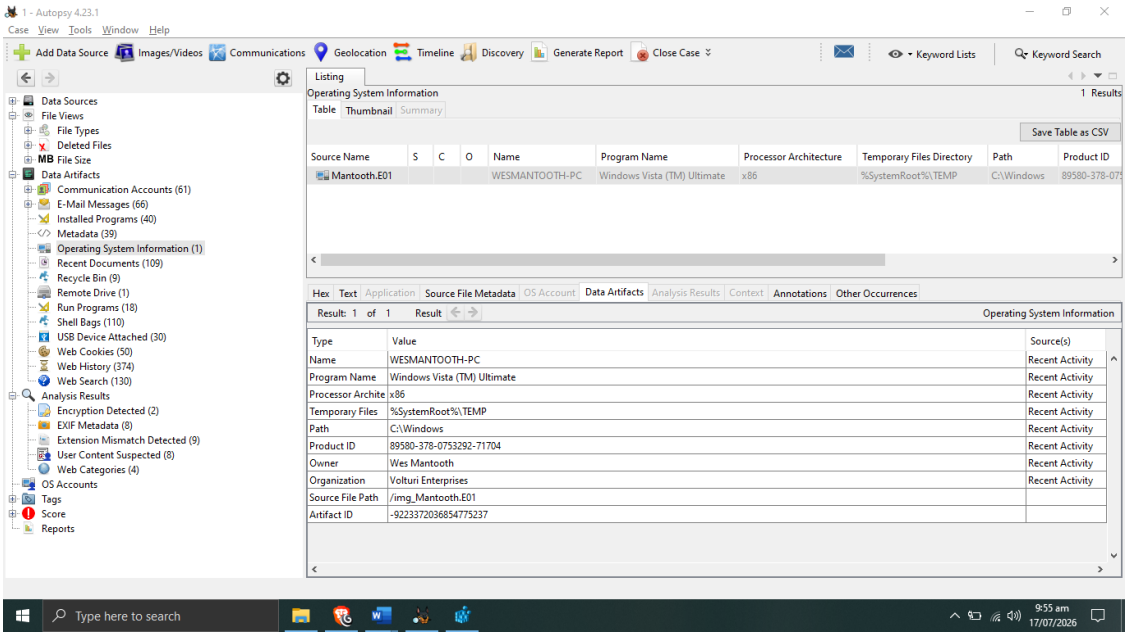


Figure 1. Operating System Information panel showing ComputerName in Autopsy.

Source 2: RegRipper (SYSTEM hive)

Result: ComputerName = WESMANTOOTH-PC; TCP/IP Hostname = WesMantooth-PC.

```
compname v.20090727
(System) Gets ComputerName and Hostname values from System hive

ComputerName    = WESMANTOOTH-PC
TCP/IP Hostname = WesMantooth-PC
```

Figure 2. compname plugin output confirming the ComputerName value independently.

Source 3: Host Registry Comparison

Result: Same key structure confirmed on the comparison host (value not disclosed for the examiner's personal device).

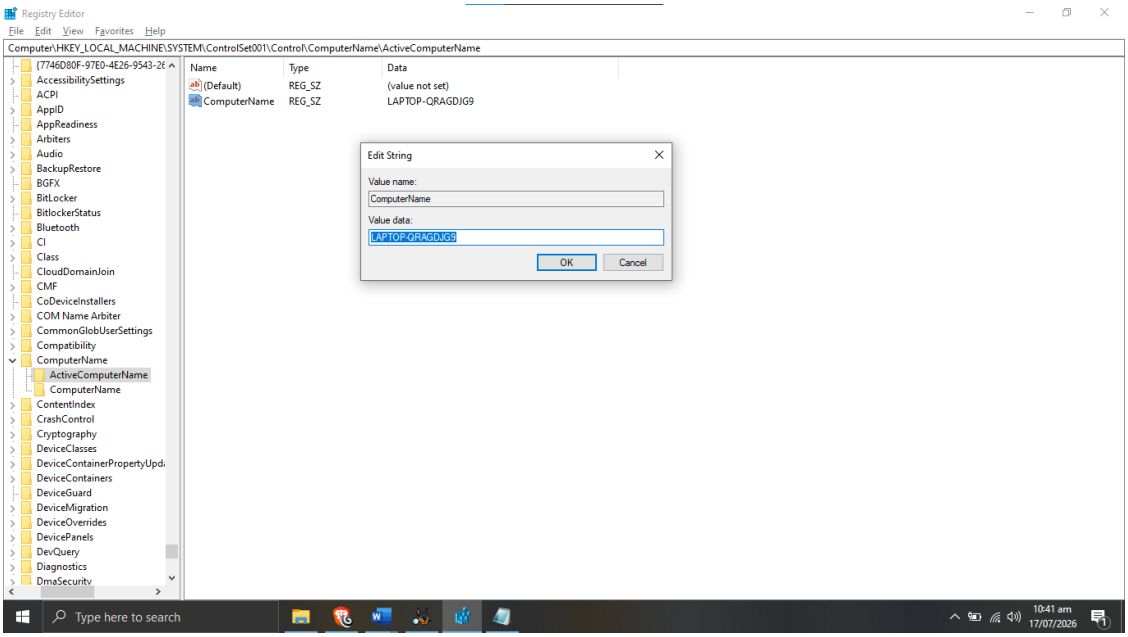


Figure 3. Equivalent ComputerName key located on the host system.

Finding 2, System Time Zone

Purpose: Confirms the system's configured time zone so every other timestamp recovered in this examination can be converted to a common reference and compared accurately.

Source 1: Autopsy

Registry path: `SYSTEM\ControlSet001\Control\TimeZoneInformation`

Result: Data-source timezone tag: Asia/Karachi (examiner's ingest setting for the case).

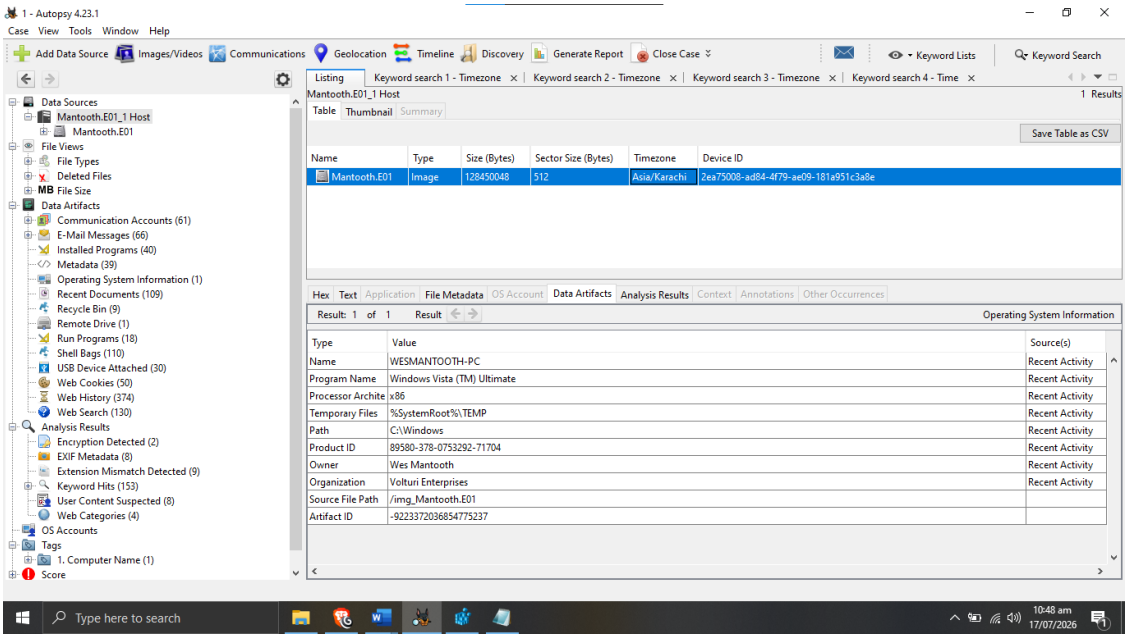


Figure 4. Data source properties and image metadata in Autopsy.

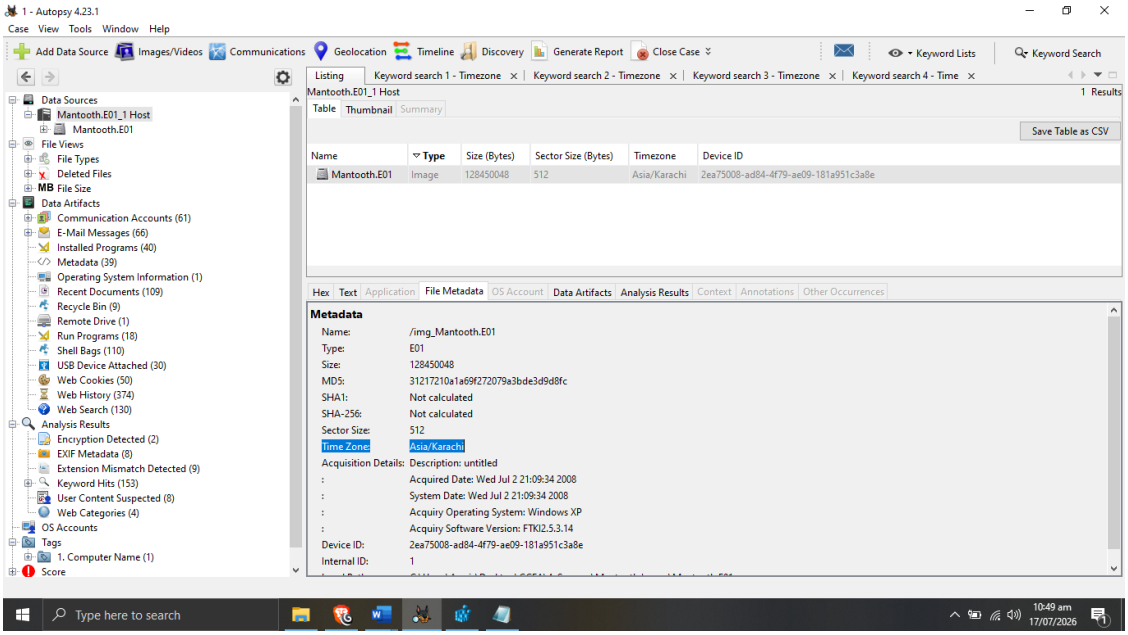


Figure 5. Data source properties and image metadata in Autopsy.

Source 2: RegRipper (SYSTEM hive)

Result: TimeZoneKeyName = Mountain Standard Time; Bias = 420 minutes (UTC-7); LastWrite 2007-03-26 15:04:03Z.

```
timezone v.20200518
(System) Get TimeZoneInformation key contents

TimeZoneInformation key
ControlSet001\Control\TimeZoneInformation
LastWrite Time 2007-03-26 15:04:03Z
  DaylightName   -> @tzres.dll,-191
  StandardName   -> @tzres.dll,-192
  Bias           -> 420 (7 hours)
  ActiveTimeBias -> 360 (6 hours)
  TimeZoneKeyName-> Mountain Standard Time me  ime   ┌▯   ▯ ▯pH ▯p皴瘻▯鵁••▯厳▯厳   焙理▯η          ▯η   ▯p¤厳焙理▯η η    ▯p▯p▯8焙理▯η      η ▯p〰厳▯η      η ア•   ▯p
```

Figure 6. timezone plugin output decoding TimeZoneInformation.

Source 3: Host Registry Comparison

Result: Comparison host is configured for Pakistan Standard Time, confirms the key decodes correctly outside the evidence file.

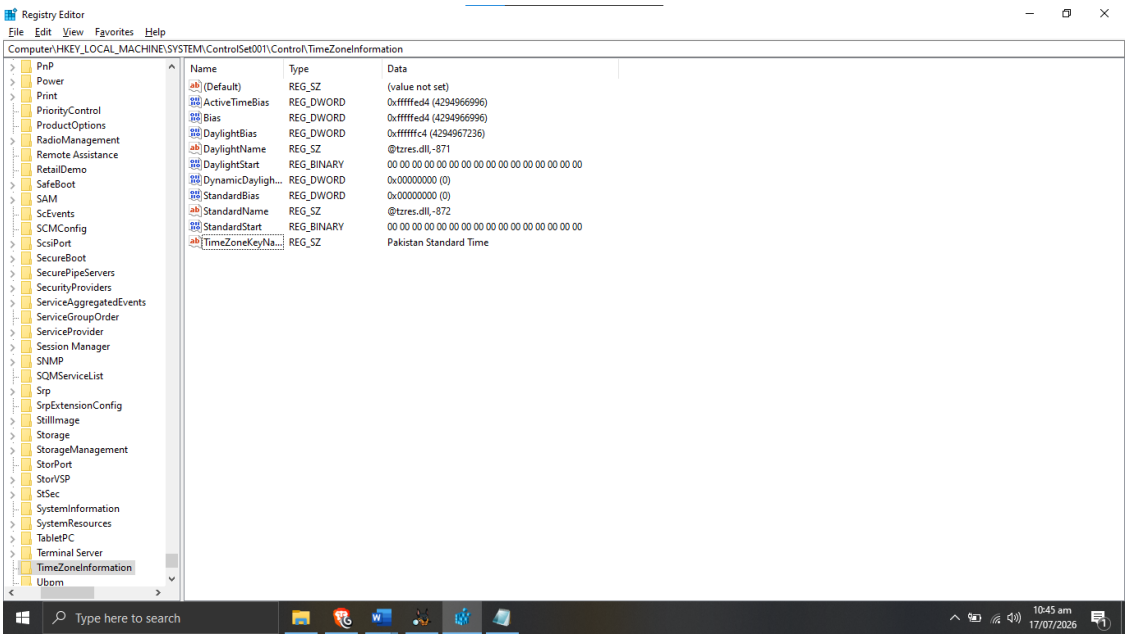


Figure 7. TimeZoneInformation key on the host system.

EVIDENCE NOTE: FORENSIC SIGNIFICANCE

The registry's TimeZoneInformation (Mountain Standard Time, UTC-7) is the system-configured zone and is distinct from Autopsy's Asia/Karachi tag, which only reflects the examiner's ingest/display setting, a useful reminder to always convert timestamps against the artifact's own recorded zone, not the analysis workstation's.

Finding 3, IDE Hard Drive Enumeration

Purpose: Attempts to identify the system's internal storage controller/disk enumeration, to build a complete hardware inventory of the machine.

Examiner's note: the screenshots captured for this item in the original worksheet document USB mass-storage enumeration (USBSTOR) rather than the SYSTEM\Enum\IDE branch. They are reported below exactly as captured, with the mismatch flagged rather than silently corrected.

Source 1: Autopsy

Registry path: `SYSTEM\ControlSet001\Enum\IDE  (not directly captured, see note above)`

Result: View captured shows the case data-source summary rather than an IDE controller entry.

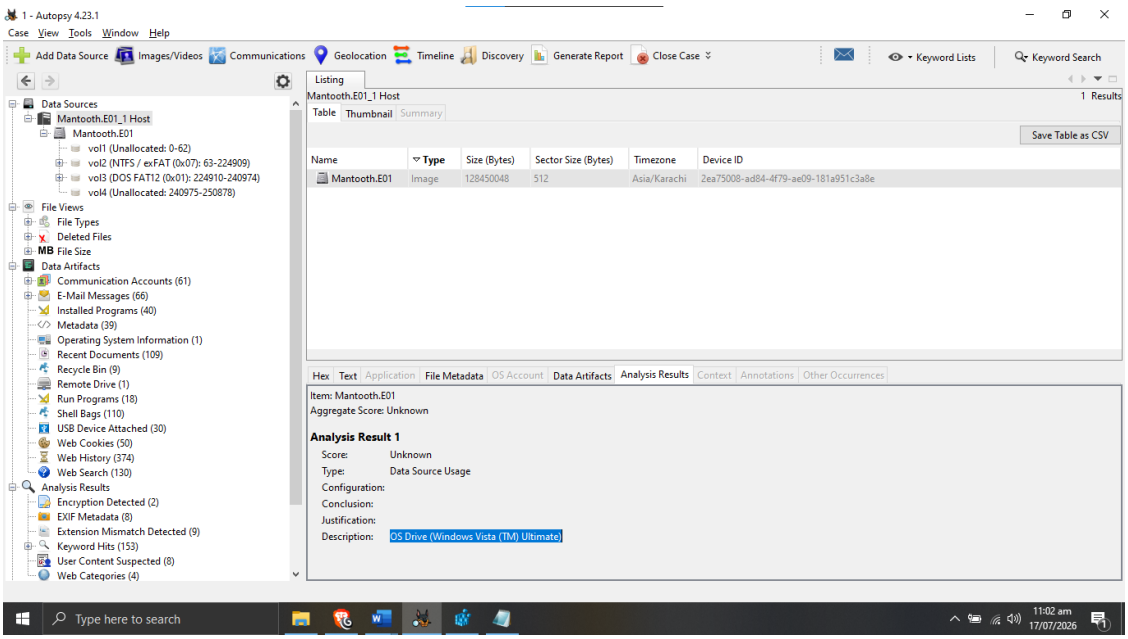


Figure 8. Data source summary and USB Device Attached listing captured under this item.

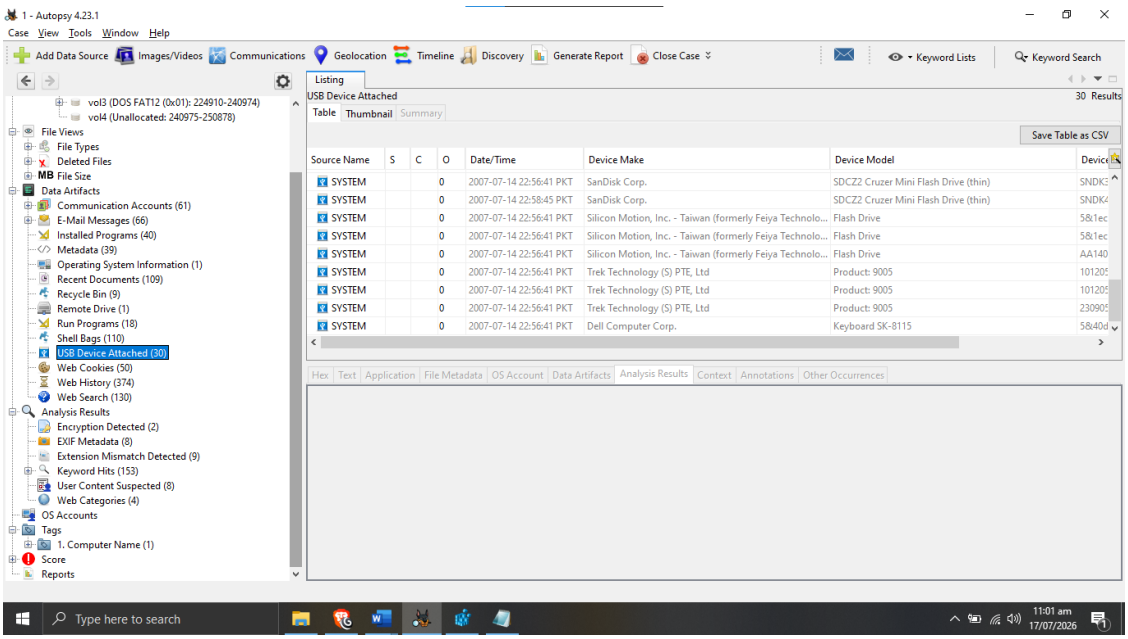


Figure 9. Data source summary and USB Device Attached listing captured under this item.

Source 2: RegRipper (SYSTEM hive)

Result: usbstor plugin output: "General UDisk USB Device" and related USBSTOR entries, not an IDE/ATA device string.

```
usbstor v.20200515
(System) Get USBStor key info

USBStor
ControlSet001\Enum\USBStor

Disk&Ven_Apple&Prod_iPod&Rev_1.62 [2007-07-14 17:56:41]
  S/N: 000A270014B302AB&0 [2007-07-14 17:56:41Z]
  Device Parameters LastWrite: [2007-07-14 17:56:41Z]
  LogConf LastWrite          : [2007-07-14 17:56:41Z]
  Properties LastWrite       : [2007-07-14 17:56:41Z]
    FriendlyName          : Apple iPod USB Device

Disk&Ven_Flash&Prod_Drive_SM_USB20&Rev_1000 [2007-07-14 17:56:41]
  S/N: 6&6b8c30&0&AA14012714842&0 [2007-07-14 17:56:41Z]
  Device Parameters LastWrite: [2007-07-14 17:56:41Z]
  LogConf LastWrite          : [2007-07-14 17:56:41Z]
  Properties LastWrite       : [2007-07-14 17:56:41Z]
    FriendlyName          : Flash Drive SM_USB20 USB Device
  S/N: AA14012714842&0 [2007-07-14 17:56:41Z]
  Device Parameters LastWrite: [2007-07-14 17:56:41Z]
  LogConf LastWrite          : [2007-07-14 17:56:41Z]
  Properties LastWrite       : [2007-07-14 17:56:41Z]
    FriendlyName          : Flash Drive SM_USB20 USB Device

Disk&Ven_Flash&Prod_Drive_UT_USB20&Rev_0.00 [2007-07-14 17:56:41]
  S/N: 0000000000C80F&0 [2007-07-14 17:56:41Z]
  Device Parameters LastWrite: [2007-07-14 17:56:41Z]
  LogConf LastWrite          : [2007-07-14 17:56:41Z]
  Properties LastWrite       : [2007-07-14 17:56:41Z]
    FriendlyName          : Flash Drive UT_USB20 USB Device
  S/N: 0000000000C9BA&0 [2007-07-14 17:56:41Z]
  Device Parameters LastWrite: [2007-07-14 17:56:41Z]
  LogConf LastWrite          : [2007-07-14 17:56:41Z]
  Properties LastWrite       : [2007-07-14 17:56:41Z]
    FriendlyName          : Flash Drive UT_USB20 USB Device
```

Figure 10. usbstor plugin output captured under this item.

Source 3: Host Registry Comparison

Result: USBSTOR\Disk&Ven_General&Prod_UDisk&Rev_5.00 key structure shown for comparison.

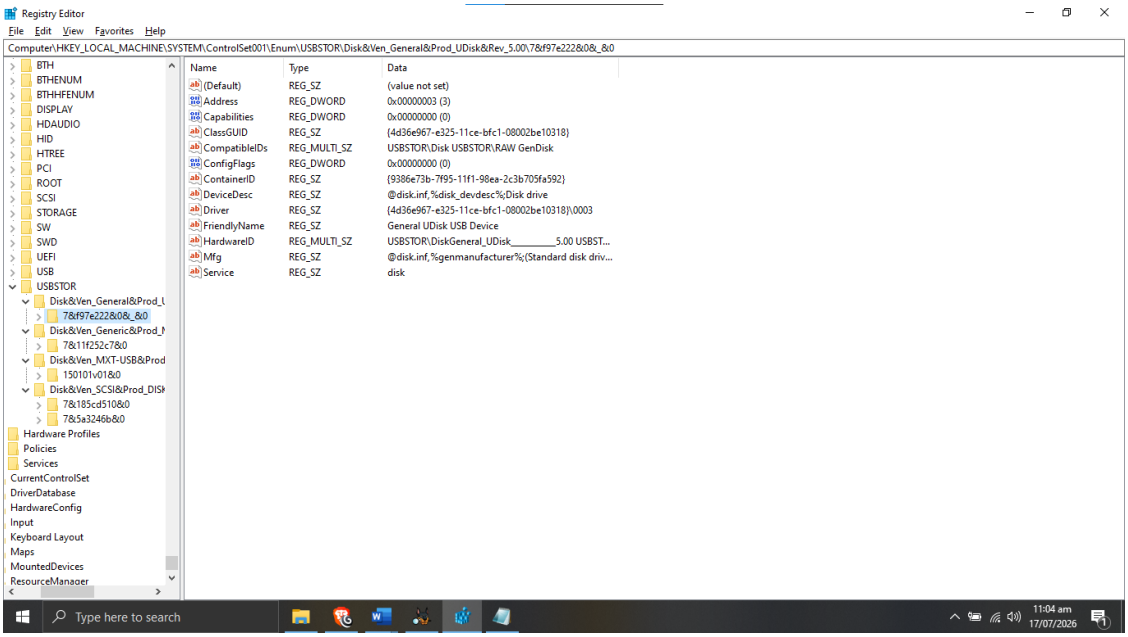


Figure 11. USBSTOR key on the host system.

Finding 4, Configured IP Address / DHCP Information

Purpose: Identifies the network configuration in effect at the time of the image, which is a prerequisite for interpreting any network-related artifacts.

Source 1: Autopsy

Registry path: `SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{37D092BF-ED97-466D-AF27-CA19AAFDCC17}`

Result: DhcpIPAddress = 172.60.33.130; DhcpServer = 172.60.60.1; Domain hint decodes to a comcast.net DHCP lease.

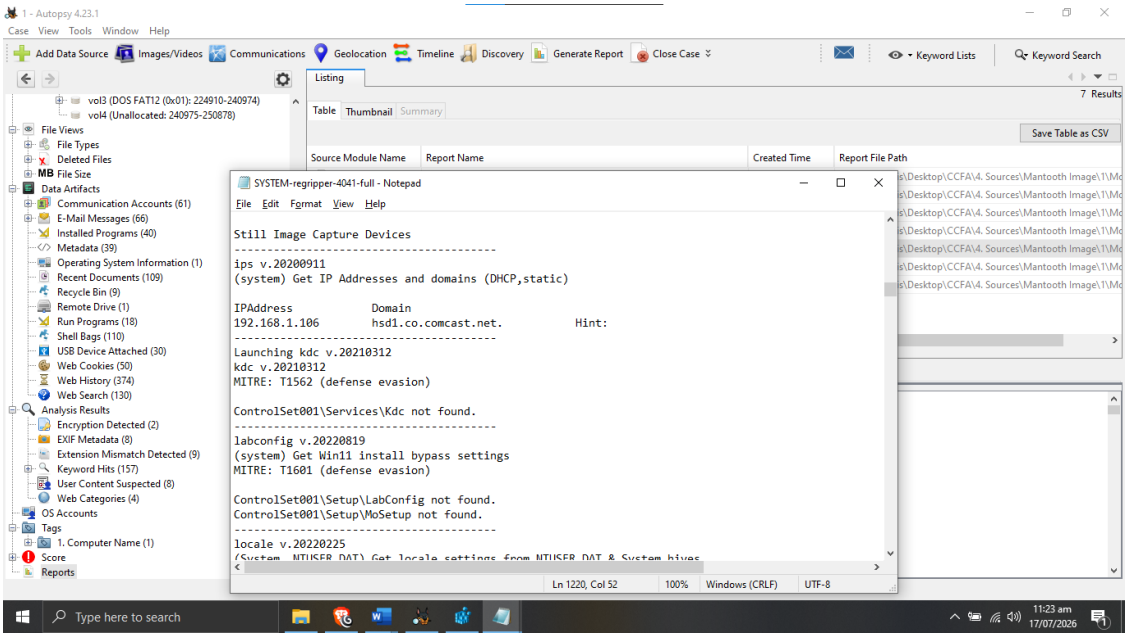


Figure 12. RegRipper report browsed inside Autopsy, and the Tcpip\Parameters\Interfaces enumeration.

Source 2: RegRipper (SYSTEM hive)

Result: IPAddress 192.168.1.106, Domain hsd1.co.comcast.net (ips plugin, resolved DHCP-assigned address and ISP domain).

```
ips v.20200518
(System) Get IP Addresses and domains (DHCP,static)

IPAddress            Domain
192.168.1.106        hsd1.co.comcast.net.          Hint:
```

Figure 13. ips plugin output listing the IP address and DHCP domain.

Source 3: Host Registry Comparison

Result: Equivalent DHCP-leased interface parameters located for structural comparison (value not disclosed for the examiner's personal network).

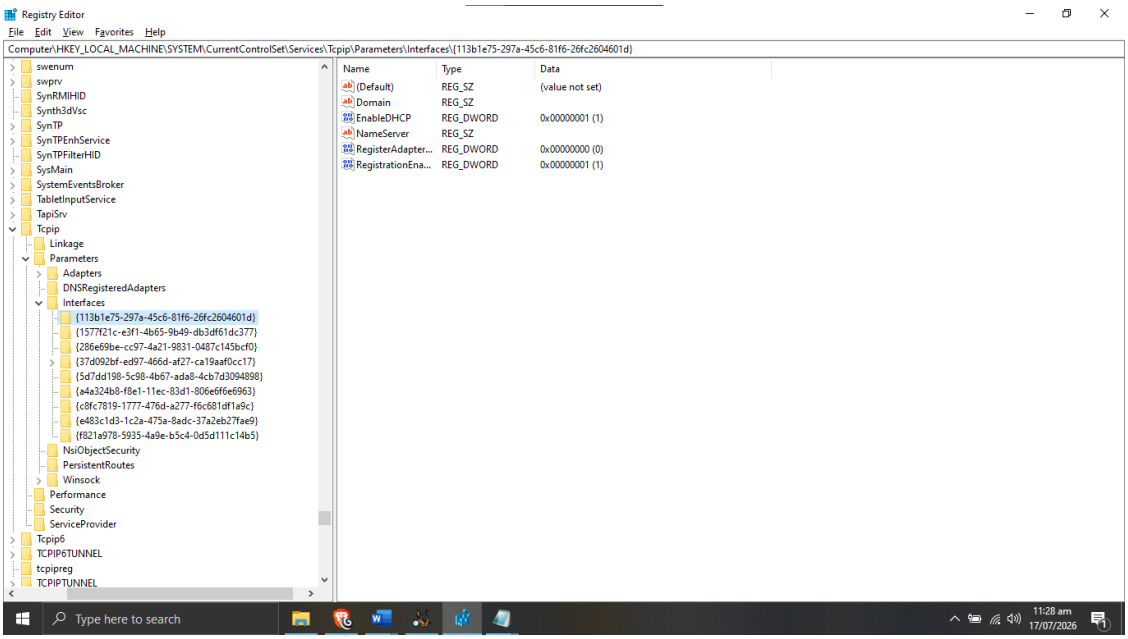


Figure 14. Tcpip\Parameters\Interfaces key on the host system.

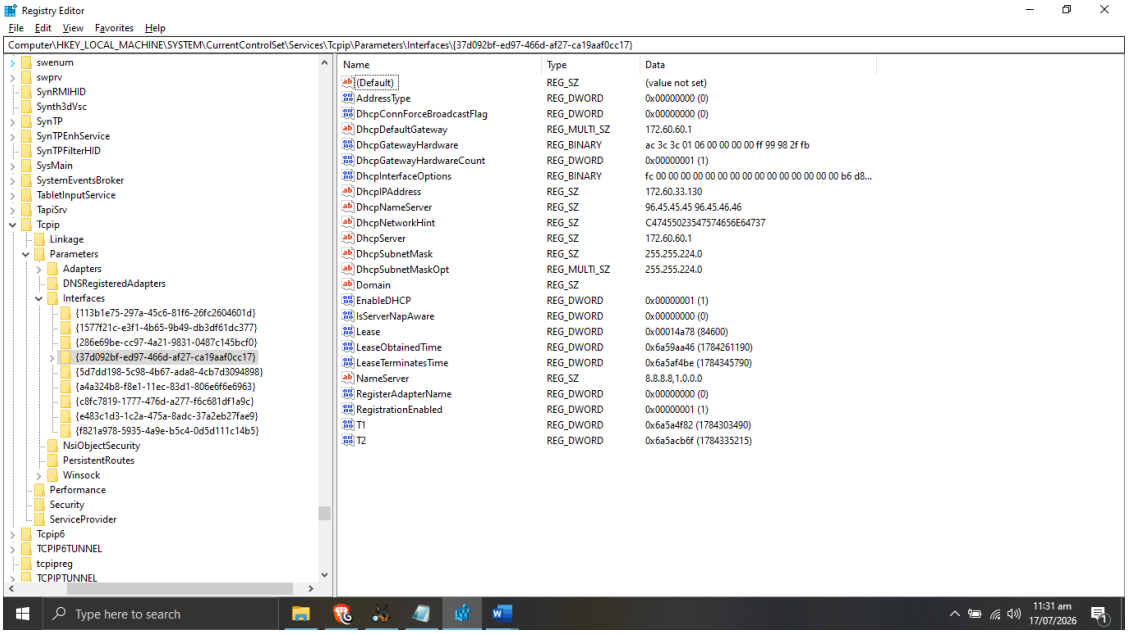


Figure 15. Tcpip\Parameters\Interfaces key on the host system.

Finding 5, Prefetch Parameters (EnablePrefetcher) Setting

Purpose: Confirms whether Windows Prefetch was enabled, which determines whether Prefetch (.pf) files are a reliable secondary source of program-execution evidence later in this examination.

Source 1: Autopsy

Registry path: `SYSTEM\ControlSet001\Control\Session Manager\Memory Management\PrefetchParameters`

Result: EnablePrefetcher = 3 (both boot and application prefetching enabled).

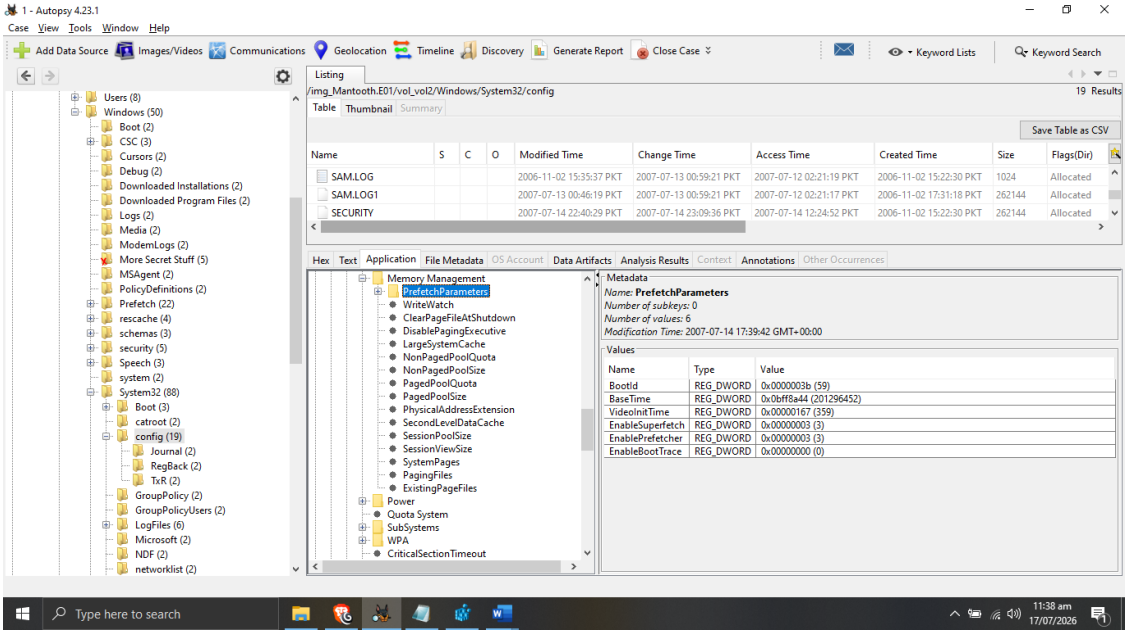


Figure 16. PrefetchParameters key values in Autopsy's registry viewer.

Source 2: RegRipper (SYSTEM hive)

Result: EnablePrefetcher = 3, confirming boot + application prefetching, meaning Prefetch (.pf) files were actively being written for executed programs.

```
-----------------------------------------
prefetch v.20200515
(System) Gets the the Prefetch Parameters

EnablePrefetcher    = 3

0 = Prefetching is disabled
1 = Application prefetching is enabled
2 = Boot prefetching is enabled
3 = Both boot and application prefetching is enabled
```

Figure 17. prefetch plugin output and its value legend.

Source 3: Host Registry Comparison

Result: EnablePrefetcher = 3 on the comparison host as well (Windows default on most desktop builds).

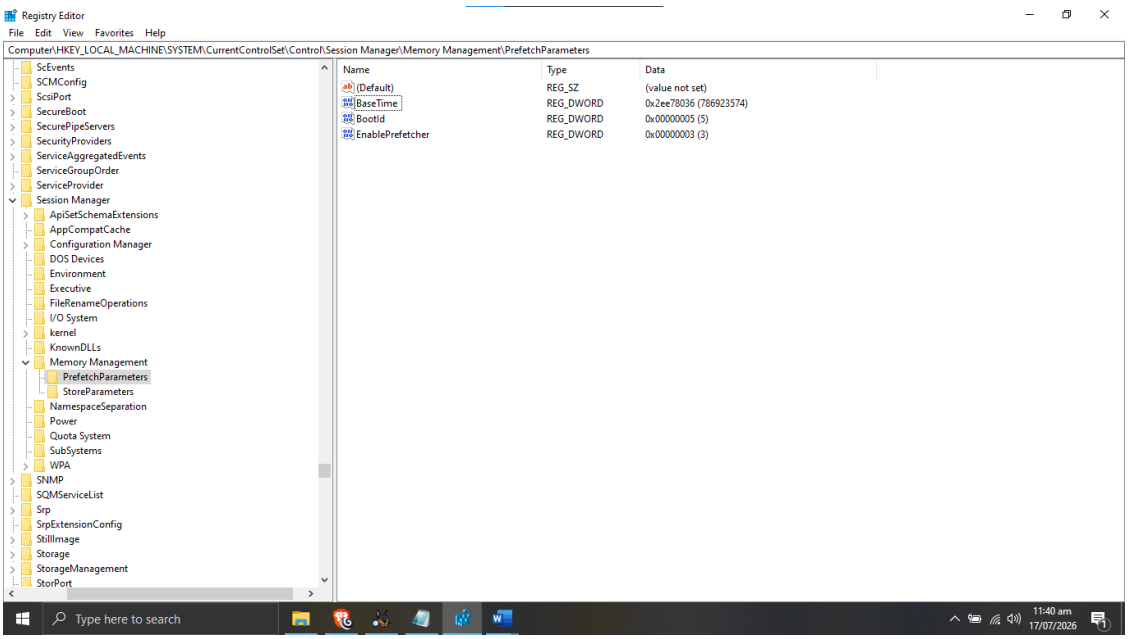


Figure 18. PrefetchParameters key on the host system.

> **EVIDENCE NOTE: FORENSIC SIGNIFICANCE**
>
> Because prefetching was enabled for applications (not just boot), the Prefetch folder is a reliable secondary source of program-execution evidence for this case, it is what makes the BESTCRYPT.EXE execution evidence in Finding 30 possible to recover.

Finding 6, TrueCrypt Service Start Type

Purpose: Determines whether the disk-encryption utility TrueCrypt was installed and how its driver was configured to load, which is directly relevant to a case narrative involving concealment of data.

Source 1: Autopsy

Registry path: `SYSTEM\ControlSet001\Services\truecrypt`

Result: Start = 0x00000001 (1), “System” start type, loaded by the I/O manager during kernel initialization, immediately after boot-start drivers.

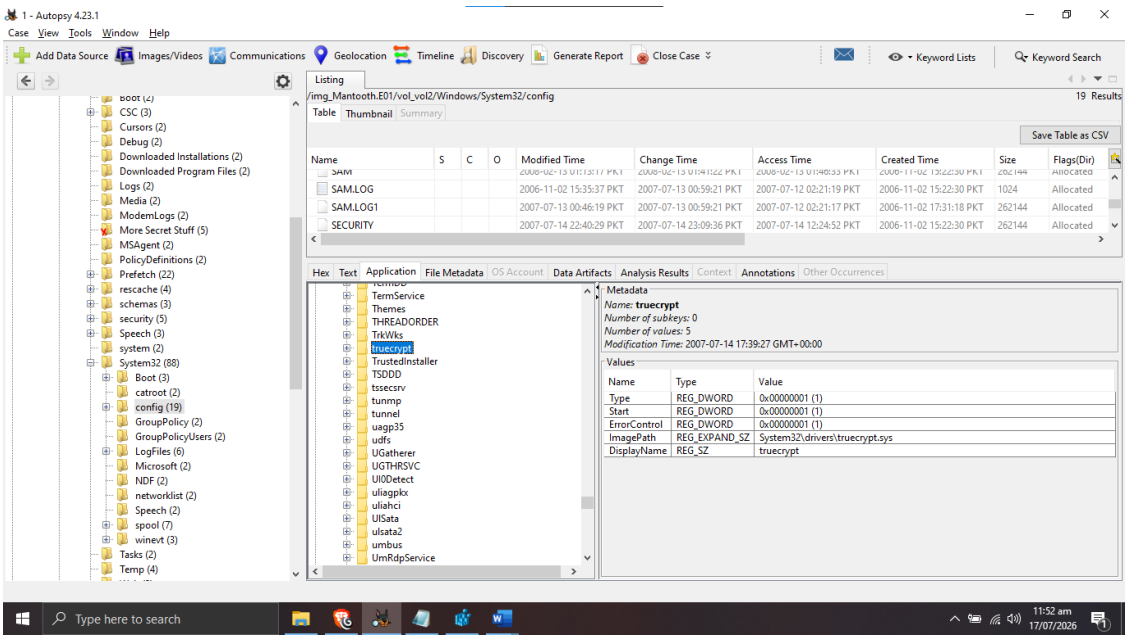


Figure 19. truecrypt service key and its Start value in Autopsy.

Source 2: RegRipper (SYSTEM hive)

Result: Name/Display = truecrypt; ImagePath = System32\drivers\truecrypt.sys; Type = Kernel driver.

```
Name      = truecrypt
Display   = truecrypt
ImagePath = System32\drivers\truecrypt.sys
Type      = Kernel driver
Start     = System Start
Group     =
```

Figure 20. services plugin output for the truecrypt driver entry.

Source 3: Host Registry Comparison

No truecrypt service key exists in the host system's registry: the software is not installed on the comparison machine, confirming the service key is specific to evidence handling on the Mantooth system.

> **EVIDENCE NOTE: FORENSIC SIGNIFICANCE**
>
> A registered TrueCrypt service, regardless of Start value, confirms the software was installed on the Mantooth system, directly relevant to a case narrative involving concealment of financial data.
>
> A System-start driver loads automatically at every boot, but the volume itself must still be manually mounted with a password; this is consistent with an encrypted container the user opens deliberately rather than an always-mounted system volume.
>
> Next step: correlate this service entry with Prefetch/UserAssist evidence of truecrypt.exe execution and search unallocated space for .tc container files or a hidden volume header.

Finding 7, Last Recorded System Shutdown Time

Purpose: Establishes the last time the system was cleanly shut down, providing a boundary for the period of legitimate system use.

Source 1: Autopsy

Registry path: `SYSTEM\ControlSet001\Control\Windows (ShutdownTime)`

Result: Not clearly resolved from Autopsy's generic registry viewer for this key, a legible ShutdownTime value could not be confirmed from this view alone.

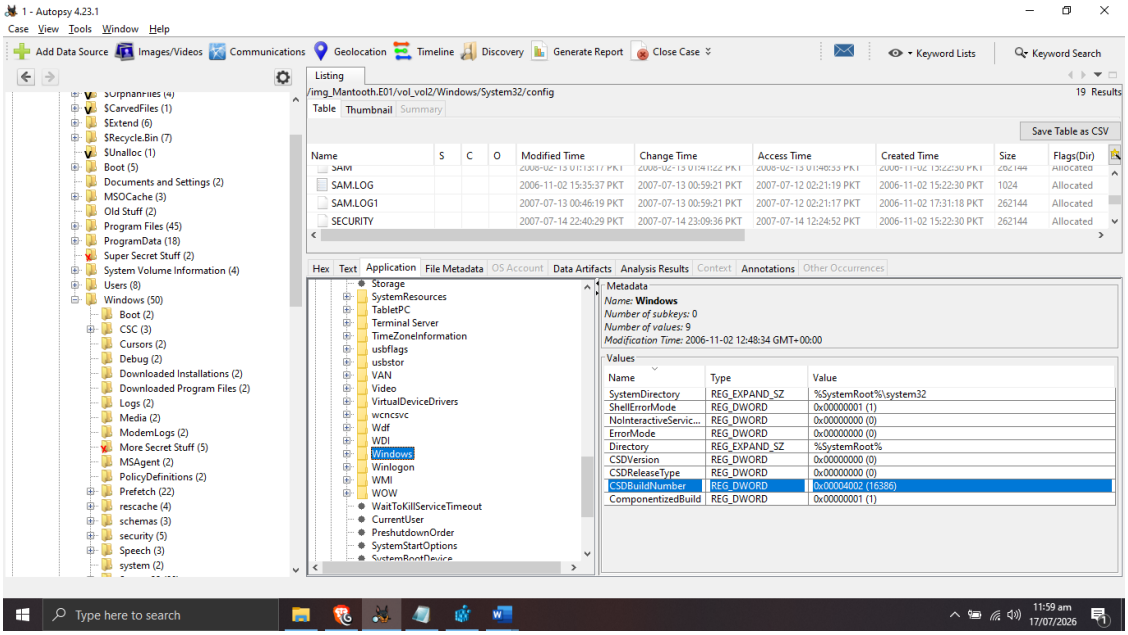


Figure 21. Windows key browsed in Autopsy, ShutdownTime not clearly rendered in this view.

Source 2: RegRipper (SYSTEM hive)

Result: Decoded value: 2006-11-02 12:48:34 UTC.

```
shutdown v.20200518
(System) Gets ShutdownTime value from System hive

ControlSet001\Control\Windows key, ShutdownTime value
LastWrite time: 2006-11-02 12:48:34Z
```

Figure 22. shutdown plugin output decoding the ShutdownTime FILETIME value.

Source 3: Host Registry Comparison

Result: Windows key located on the host system for structural comparison; no ShutdownTime value is currently set on the comparison host at the time of capture.

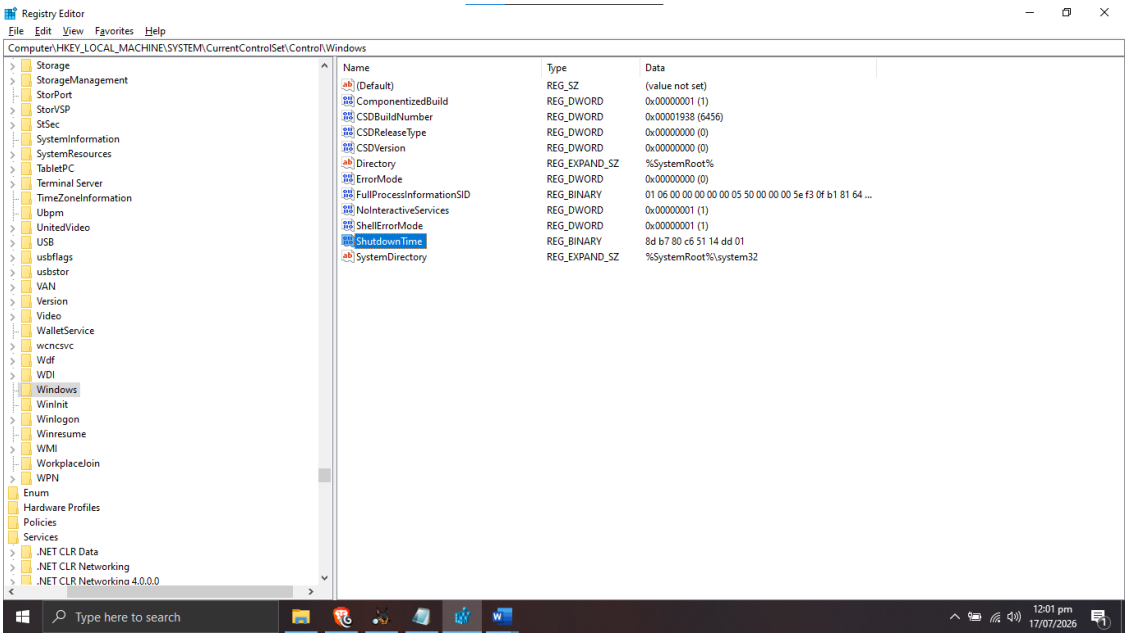


Figure 23. Windows key on the host system's SYSTEM hive.

EVIDENCE NOTE: FORENSIC SIGNIFICANCE

> SYSTEM\...\Windows\ShutdownTime stores a FILETIME written on every clean shutdown and is one of the few registry values that updates automatically without user interaction, making it useful for bounding the last known period of legitimate system use, here, 2006-11-02, which is earlier than the bulk of the user-activity evidence (2007–2008) recovered elsewhere in this examination.
>
> Because Autopsy's generic viewer did not clearly surface this value, RegRipper's targeted plugin was the more reliable source: a good illustration of why single-tool findings should be corroborated rather than accepted at face value.
>
> In an active investigation this timestamp would be cross-referenced against Windows Event Log shutdown/restart events (Event ID 1074/6006) to confirm consistency.

Finding 8, Canon PowerShot SD500: Device Serial / Connection Time

Purpose: Identifies a specific USB-connected digital camera and when it was first connected, a possible source of evidence photographs relevant to the case.

Source 1: Autopsy

Registry path: `SYSTEM\ControlSet001\Enum\USBSTOR`

Result: Device Model: “Digital IXUS 700 (normal mode) / Digital IXUS 700 (PTP mode) / IXY Digital 600 (normal mode) / PowerShot SD500 (normal mode) / PowerShot SD500 (PTP mode)”; Device ID 5&1ec84238&0&4; connected 2007-07-14 22:56:41 PKT (= 17:56:41 UTC).

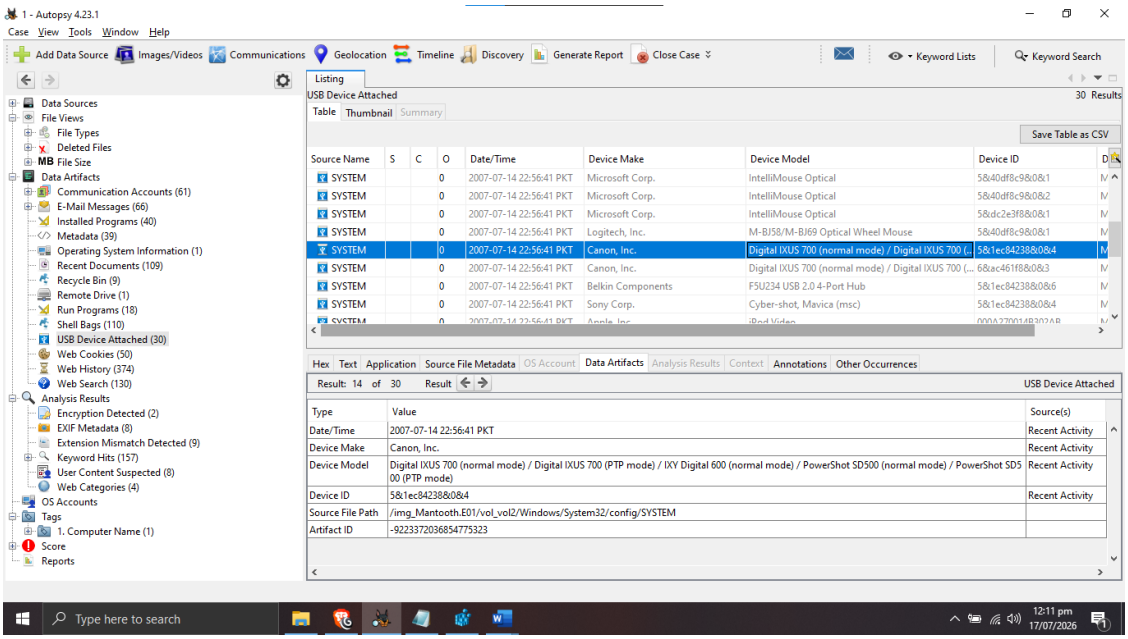


Figure 24. USB Device Attached entry for the Canon device in Autopsy.

Source 2: RegRipper (SYSTEM hive)

Result: Serial numbers 5&1ec84238&0&4 and 6&ac461f8&0&3, both first connected 2007-07-14 17:56:41Z; FriendlyName “Canon PowerShot SD500”.

```
----------------------------------------
usbdevices v.20200525
(System) Parses Enum\USB key for USB & WPD devices

VID_0457&PID_0151
LastWrite: 2007-07-14 17:56:41Z
  SN       : 0000000000C80F
  LastWrite: 2007-07-14 17:56:41Z

VID_0457&PID_0151
LastWrite: 2007-07-14 17:56:41Z
  SN       : 0000000000C9BA
  LastWrite: 2007-07-14 17:56:41Z

VID_04A9&PID_30F2
LastWrite: 2007-07-14 17:56:41Z
  SN       : 5&1ec84238&0&4
  LastWrite: 2007-07-14 17:56:41Z
MFG       : Canon Inc.
FriendlyName: Canon PowerShot SD500

VID_04A9&PID_30F2
LastWrite: 2007-07-14 17:56:41Z
  SN       : 6&ac461f8&0&3
  LastWrite: 2007-07-14 17:56:41Z
MFG       : Canon Inc.
FriendlyName: Canon PowerShot SD500
```

Figure 25. usbdevices/usbstor plugin output for the Canon PowerShot SD500.

```
VID_04A9&PID_30F2 [2007-07-14 17:56:41Z]
  S/N: 5&1ec84238&0&4 [2007-07-14 17:56:41Z]
  Properties Key LastWrite: 2007-07-14 17:56:41Z
    FriendlyName    : Canon PowerShot SD500
  S/N: 6&ac461f8&0&3 [2007-07-14 17:56:41Z]
  Properties Key LastWrite: 2007-07-14 17:56:41Z
    FriendlyName    : Canon PowerShot SD500
```

Figure 26. usbdevices/usbstor plugin output for the Canon PowerShot SD500.

Source 3: Host Registry Comparison

Not applicable: no Canon PowerShot device has ever been connected to the comparison host.

> **EVIDENCE NOTE: FORENSIC SIGNIFICANCE**
>
> USBSTOR container IDs and the associated device class GUID uniquely identify a physical device connected to this machine, and the parent key's LastWrite time approximates when it was last first connected.
>
> A digital camera is a plausible vector for both evidence photographs and, in an ATM-fraud narrative, images of card skimmers or ATM interiors, which is worth timelining against the file-system creation dates of any image files recovered from the same period.

Finding 9, Five Portable Devices Connected to the System

Purpose: Builds a complete inventory of portable/USB devices ever connected to the system, to identify every potential data-exfiltration or evidence-carrying device.

Source 1: Autopsy

Registry path: `SYSTEM\ControlSet001\Enum\USBSTOR`

Result: (1) Microsoft IntelliMouse Optical; (2) Logitech M-BJ69 Optical Wheel Mouse; (3) Canon Digital IXUS 700 / PowerShot SD500; (4) Belkin F5U234 USB 2.0 4-Port Hub; (5) Sony Cyber-shot/Mavica (msc), all first seen 2007-07-14 22:56:41 PKT.

USB Device Attached 30 Results

Table Thumbnail Summary

Save Table as CSV

Date/Time	Device Make	Device Model	Device ID	Data Source
2007-07-14 22:56:41 PKT	Canon, Inc.	Digital IXUS 700 (normal mode) / Digital IXUS 700 (PTP...	6&ac461f8&0&3	Mantooth.E0
2007-07-14 22:56:41 PKT	Belkin Components	F5U234 USB 2.0 4-Port Hub	5&1ec84238&0&6	Mantooth.E0
2007-07-14 22:56:41 PKT	Sony Corp.	Cyber-shot, Mavica (msc)	5&1ec84238&0&4	Mantooth.E0
2007-07-14 22:56:41 PKT	Apple, Inc.	iPod Video	000A270014B302AB	Mantooth.E0
2007-07-14 22:56:41 PKT	Prolific Technology, Inc.	PL3507 ATAPI6 Bridge	8396	Mantooth.E0
2007-07-14 22:56:41 PKT	Prolific Technology, Inc.	PL3507 ATAPI6 Bridge	8B76	Mantooth.E0
2007-07-14 22:58:25 PKT	SanDisk Corp.	SDCZ2 Cruzer Mini Flash Drive (thin)	20043513310C7A22D0C8	Mantooth.E0
2007-07-14 22:56:41 PKT	SanDisk Corp.	SDCZ2 Cruzer Mini Flash Drive (thin)	SNDK3066A40516400406	Mantooth.E0

Figure 27. USB Device Attached listing in Autopsy.

Source 2: RegRipper (SYSTEM hive)

Result: usbstor plugin corroborates the same device set, including the Apple iPod (S/N 00082700148302AB) and multiple flash-storage devices, all LastWrite 2007-07-14 17:56:41Z.

```
Disk&Ven_Apple&Prod_iPod&Rev_1.62 [2007-07-14 17:56:41]
  S/N: 000A270014B302AB&0 [2007-07-14 17:56:41Z]
  Device Parameters LastWrite: [2007-07-14 17:56:41Z]
  LogConf LastWrite          : [2007-07-14 17:56:41Z]
  Properties LastWrite       : [2007-07-14 17:56:41Z]
    FriendlyName          : Apple iPod USB Device

Disk&Ven_Flash&Prod_Drive_SM_USB20&Rev_1000 [2007-07-14 17:56:41]
  S/N: 6&6b8c30&0&AA14012714842&0 [2007-07-14 17:56:41Z]
  Device Parameters LastWrite: [2007-07-14 17:56:41Z]
  LogConf LastWrite          : [2007-07-14 17:56:41Z]
  Properties LastWrite       : [2007-07-14 17:56:41Z]
    FriendlyName          : Flash Drive SM_USB20 USB Device
  S/N: AA14012714842&0 [2007-07-14 17:56:41Z]
  Device Parameters LastWrite: [2007-07-14 17:56:41Z]
  LogConf LastWrite          : [2007-07-14 17:56:41Z]
  Properties LastWrite       : [2007-07-14 17:56:41Z]
    FriendlyName          : Flash Drive SM_USB20 USB Device

Disk&Ven_Flash&Prod_Drive_UT_USB20&Rev_0.00 [2007-07-14 17:56:41]
  S/N: 0000000000C80F&0 [2007-07-14 17:56:41Z]
  Device Parameters LastWrite: [2007-07-14 17:56:41Z]
  LogConf LastWrite          : [2007-07-14 17:56:41Z]
  Properties LastWrite       : [2007-07-14 17:56:41Z]
    FriendlyName          : Flash Drive UT_USB20 USB Device
  S/N: 0000000000C9BA&0 [2007-07-14 17:56:41Z]
  Device Parameters LastWrite: [2007-07-14 17:56:41Z]
  LogConf LastWrite          : [2007-07-14 17:56:41Z]
  Properties LastWrite       : [2007-07-14 17:56:41Z]
    FriendlyName          : Flash Drive UT_USB20 USB Device

Disk&Ven_Maxtor_6&Prod_B300R0&Rev_BAH4 [2007-07-14 17:56:41]
  S/N: 8396 [2007-07-14 17:56:41Z]
  Device Parameters LastWrite: [2007-07-14 17:56:41Z]
  LogConf LastWrite          : [2007-07-14 17:56:41Z]
  Properties LastWrite       : [2007-07-14 17:56:41Z]
    FriendlyName          : Maxtor 6 B300R0 USB Device
  S/N: 8B76 [2007-07-14 17:56:41Z]
  Device Parameters LastWrite: [2007-07-14 17:56:41Z]
  LogConf LastWrite          : [2007-07-14 17:56:41Z]
  Properties LastWrite       : [2007-07-14 17:56:41Z]
    FriendlyName          : Maxtor 6 B300R0 USB Device

Disk&Ven_SanDisk&Prod_Cruzer_Mini&Rev_0.1 [2007-07-14 17:56:41]
  S/N: SNDK3066A40516400406&0 [2007-07-14 17:56:41Z]
  Device Parameters LastWrite: [2007-07-14 17:56:41Z]
  LogConf LastWrite          : [2007-07-14 17:56:41Z]
  Properties LastWrite       : [2007-07-14 17:56:41Z]
    FriendlyName          : SanDisk Cruzer Mini USB Device
```

Figure 28. usbstor plugin output enumerating connected devices.

Source 3: Host Registry Comparison

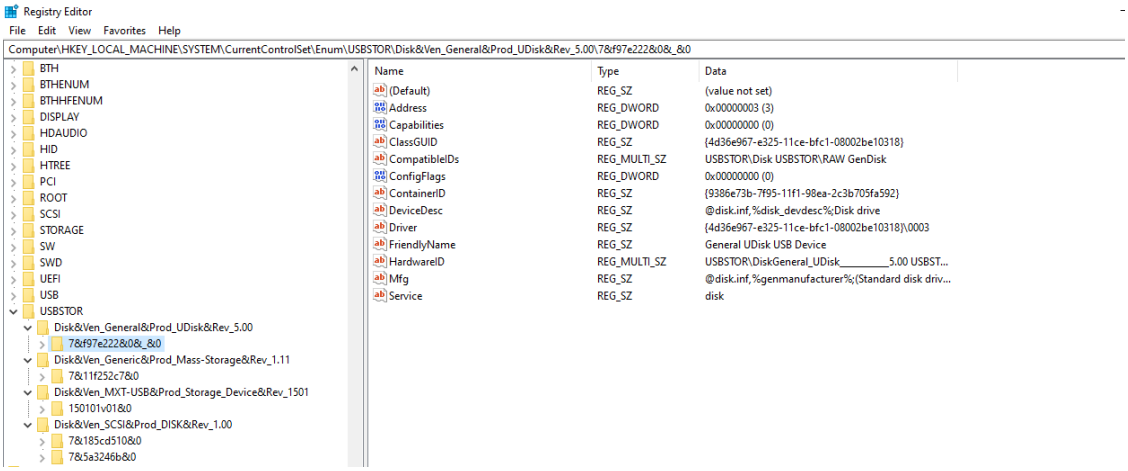


Figure 29. Portable devices recorded on the host comparison system.

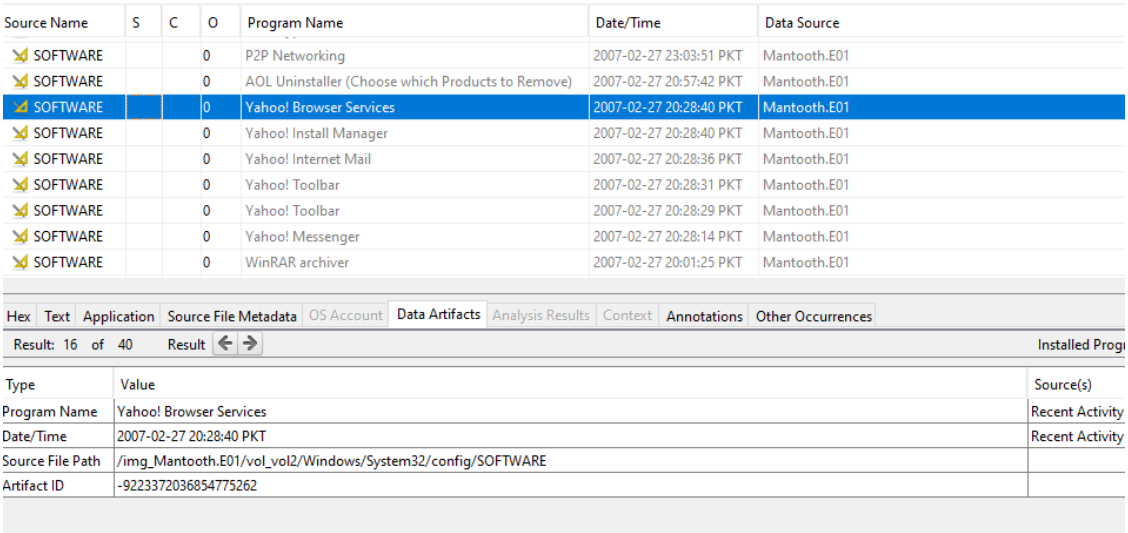
Finding 10, Default Web Browser

Purpose: Identifies which browser the user relied on by default, to help scope which browser artifacts (history, downloads, cache) are most relevant to pursue.

Examiner's note: the Autopsy screenshot captured for this item shows the Installed Programs list rather than the browser file-association key; the actual default-browser value was not independently isolated on the Mantooth image in this examination.

Source 1: Autopsy

Result: Not conclusively isolated from the captured view, installed browser-related entries include Yahoo! Browser Services, consistent with a Yahoo! toolbar/software suite, but no explicit UserChoice ProgId was captured.



Source Name	S	C	O	Program Name	Date/Time	Data Source
SOFTWARE			0	P2P Networking	2007-02-27 23:03:51 PKT	Mantooth.E01
SOFTWARE			0	AOL Uninstaller (Choose which Products to Remove)	2007-02-27 20:57:42 PKT	Mantooth.E01
SOFTWARE			0	Yahoo! Browser Services	2007-02-27 20:28:40 PKT	Mantooth.E01
SOFTWARE			0	Yahoo! Install Manager	2007-02-27 20:28:40 PKT	Mantooth.E01
SOFTWARE			0	Yahoo! Internet Mail	2007-02-27 20:28:36 PKT	Mantooth.E01
SOFTWARE			0	Yahoo! Toolbar	2007-02-27 20:28:31 PKT	Mantooth.E01
SOFTWARE			0	Yahoo! Toolbar	2007-02-27 20:28:29 PKT	Mantooth.E01
SOFTWARE			0	Yahoo! Messenger	2007-02-27 20:28:14 PKT	Mantooth.E01
SOFTWARE			0	WinRAR archiver	2007-02-27 20:01:25 PKT	Mantooth.E01

Type	Value	Source(s)
Program Name	Yahoo! Browser Services	Recent Activity
Date/Time	2007-02-27 20:28:40 PKT	Recent Activity
Source File Path	/img_Mantooth.E01/vol_vol2/Windows/System32/config/SOFTWARE	
Artifact ID	-9223372036854775262	

Figure 30. Installed Programs listing captured under this item.

Source 3: Host Registry Comparison

Registry path:
`HKCU\Software\Microsoft\Windows\Shell\Associations\UrlAssociations\http\UserChoice`

Result: ProgId decodes to Brave, confirms the UserChoice key and hashing mechanism (introduced in Windows 8+) as the modern equivalent of this artifact on the examiner's own system.

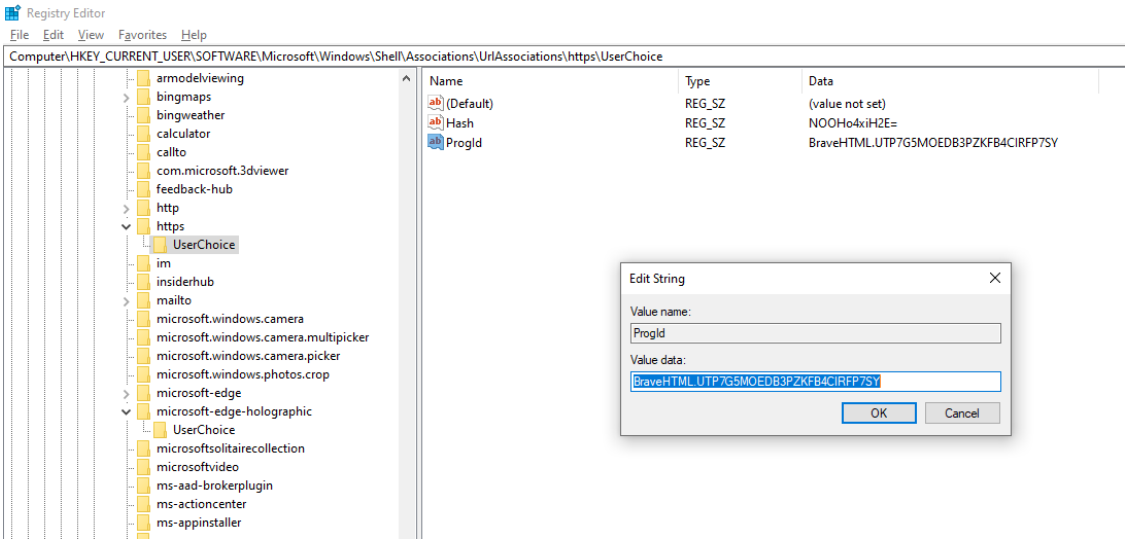


Figure 31. UserChoice key on the host system showing the Brave ProgId.

Finding 11, Network Interface Cards Installed

Purpose: Inventories the network hardware installed on the system, to understand what network paths were available to the user.

Source 1: Autopsy

Registry path: `SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards`

Result: Network Connections folder enumerated in Autopsy, corroborating the two adapters identified below.

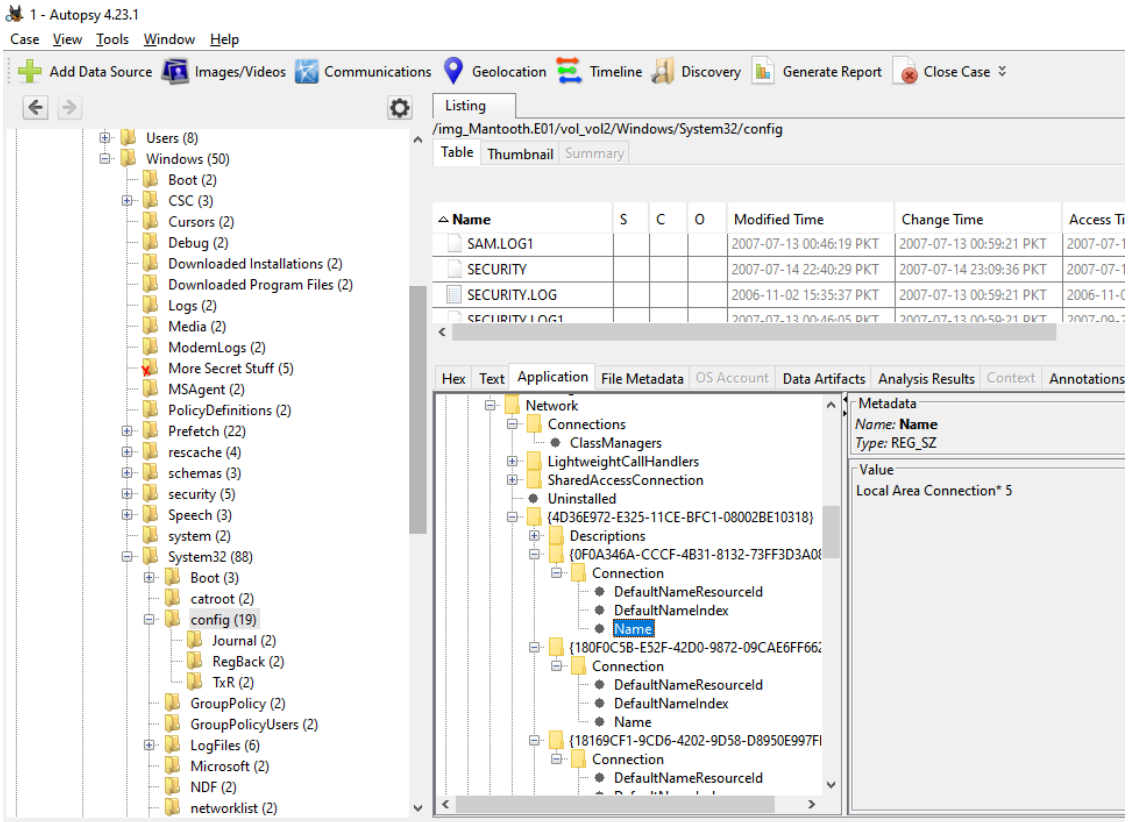


Figure 32. Network adapter enumeration in Autopsy.

Source 2: RegRipper (SOFTWARE hive)

Result: Linksys Wireless-G USB Network Adapter (key LastWrite 2008-02-12 18:14:42Z); Realtek RTL8139/810x Family Fast Ethernet NIC (key LastWrite 2007-02-27 19:21:27Z).

```
networkcards v.20200518
(Software) Get NetworkCards Info

NetworkCards
Microsoft\Windows NT\CurrentVersion\NetworkCards

Description                                        Key LastWrite time
Linksys Wireless-G USB Network Adapter             2008-02-12 18:14:42Z
Realtek RTL8139/810x Family Fast Ethernet NIC      2007-02-27 19:21:27Z
```

Figure 33. networkcards plugin output listing both adapters.

Source 3: Host Registry Comparison

Result: Host system's own NetworkCards key located for structural comparison (e.g. Realtek RTL8821CE 802.11ac PCIe Adapter).

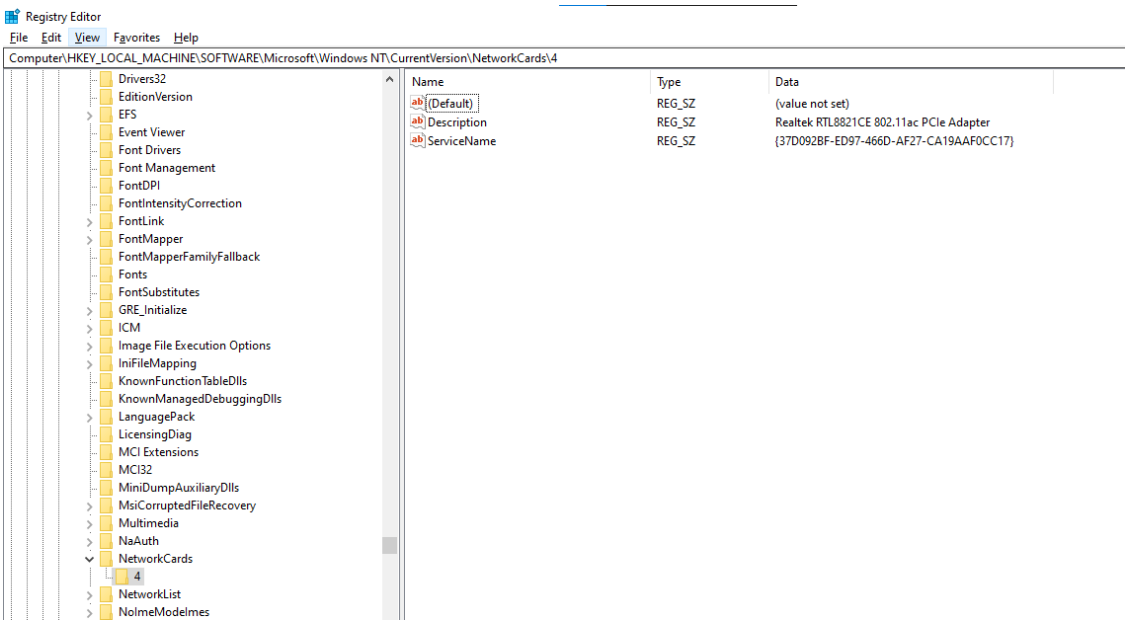


Figure 34. NetworkCards key on the host system.

Finding 12, Configured Wireless Network Profile Name

Purpose: Identifies which wireless network the system connected to, which can help corroborate a suspect's location or identify a shared network relevant to the case.

Source 1: Autopsy

Registry path: `SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{GUID}`

Among the three saved network profiles, only one carries NameType 0x47 (71 decimal), the Windows-standard indicator for an 802.11 Wireless (Wi-Fi) connection; the other two are wired (NameType 0x06).

Result: ProfileName = Frankenwave2 (NameType 0x47 / wireless; DateLastConnected 2008-02-12).

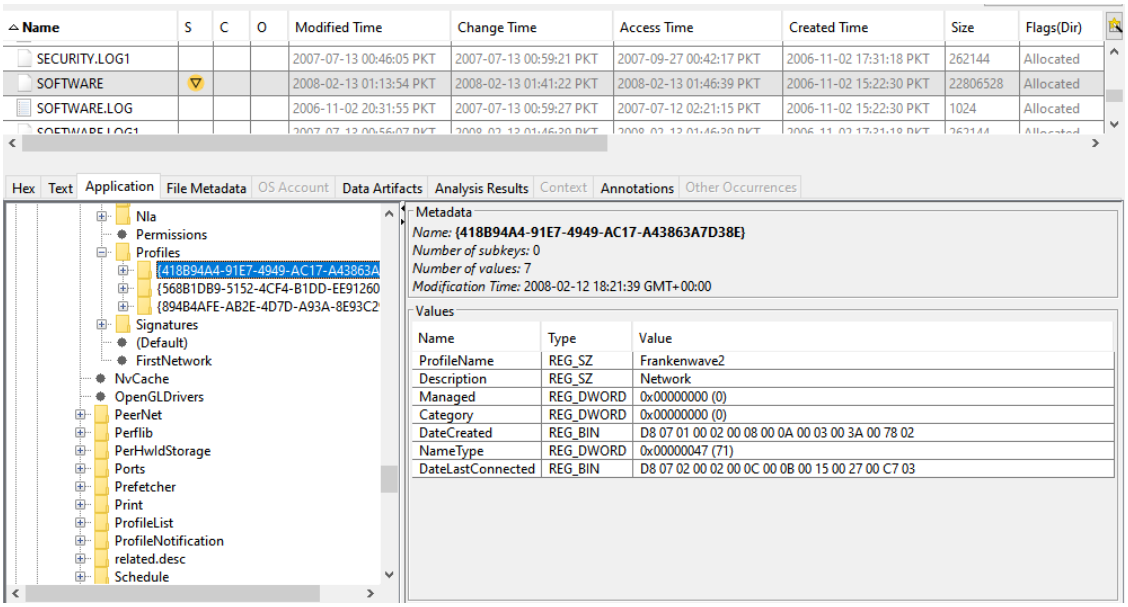


Figure 35. The three NetworkList profile keys in Autopsy, Frankenwave2, adata.com, and Network.

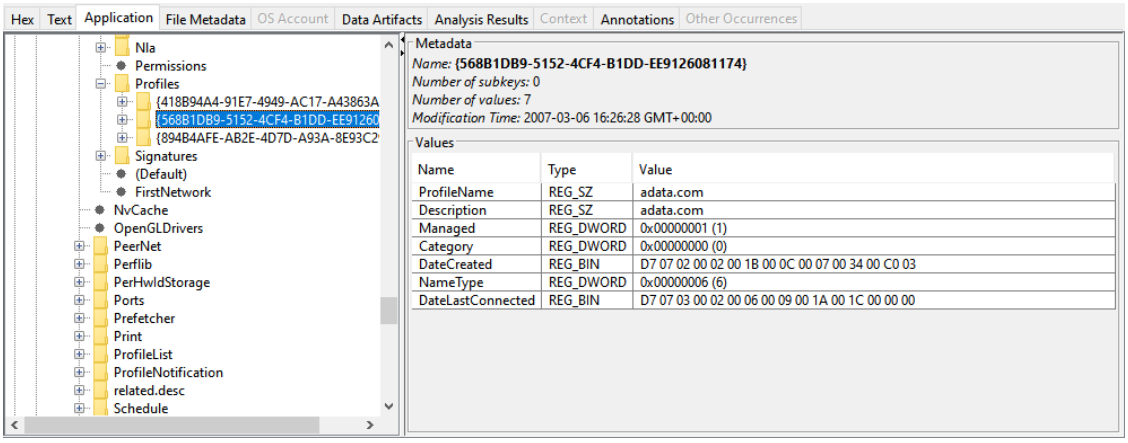


Figure 36. The three NetworkList profile keys in Autopsy, Frankenwave2, adata.com, and Network.

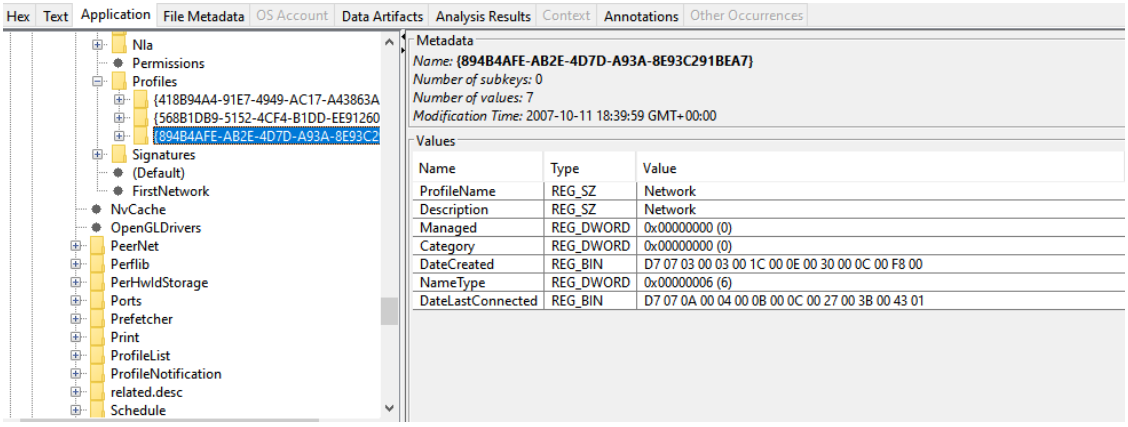


Figure 37. The three NetworkList profile keys in Autopsy, Frankenwave2, adata.com, and Network.

Source 2: RegRipper (SOFTWARE hive)

Result: networklist plugin explicitly labels Frankenwave2 as Type: wireless, distinct from the two Type: wired profiles (adata.com, Network).

```
Launching networklist v.20200518
(Software) Collects network info from NetworkList key

Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles
Frankenwave2
  Key LastWrite    : 2008-02-12 18:21:39Z
  DateLastConnected: 2008-02-12 11:21:39
  DateCreated      : 2008-01-08 10:03:58
  DefaultGatewayMac: 00-1C-F0-55-BE-E9
  Type             : wireless

adata.com
  Key LastWrite    : 2007-03-06 16:26:28Z
  DateLastConnected: 2007-03-06 09:26:28
  DateCreated      : 2007-02-27 12:07:52
  DefaultGatewayMac: 00-09-0F-04-03-A4
  Type             : wired

Network
  Key LastWrite    : 2007-10-11 18:39:59Z
  DateLastConnected: 2007-10-11 12:39:59
  DateCreated      : 2007-03-28 14:48:12
  DefaultGatewayMac: 00-0D-88-BF-5F-99
  Type             : wired


Domain/IP
adata.com
hsd1.co.comcast.net.


Nla\Wireless
Frankenwave2
```

Figure 38. networklist plugin output labeling each profile's connection type.

Source 3: Host Registry Comparison

Result: Two NameType 0x47 (wireless) profiles located on the host for comparison, confirming the same artifact structure applies on modern Windows builds.

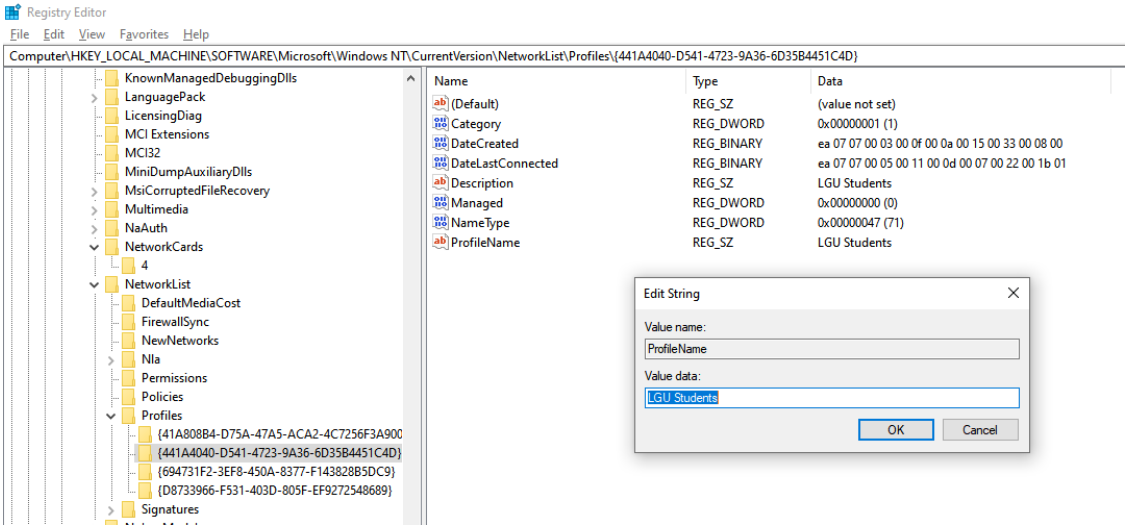


Figure 39. NetworkList profile keys on the host system.

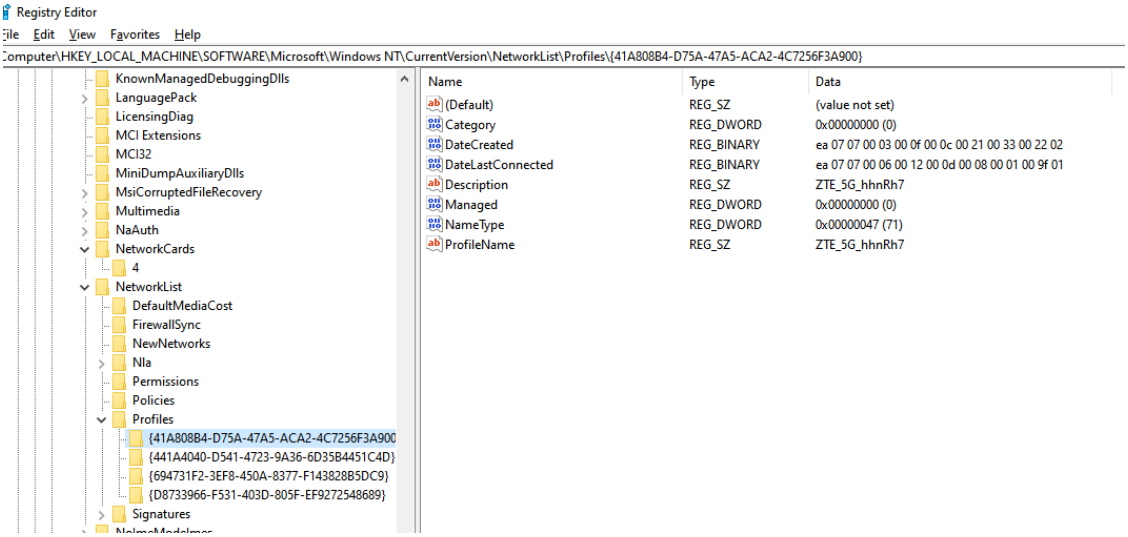


Figure 40. NetworkList profile keys on the host system.

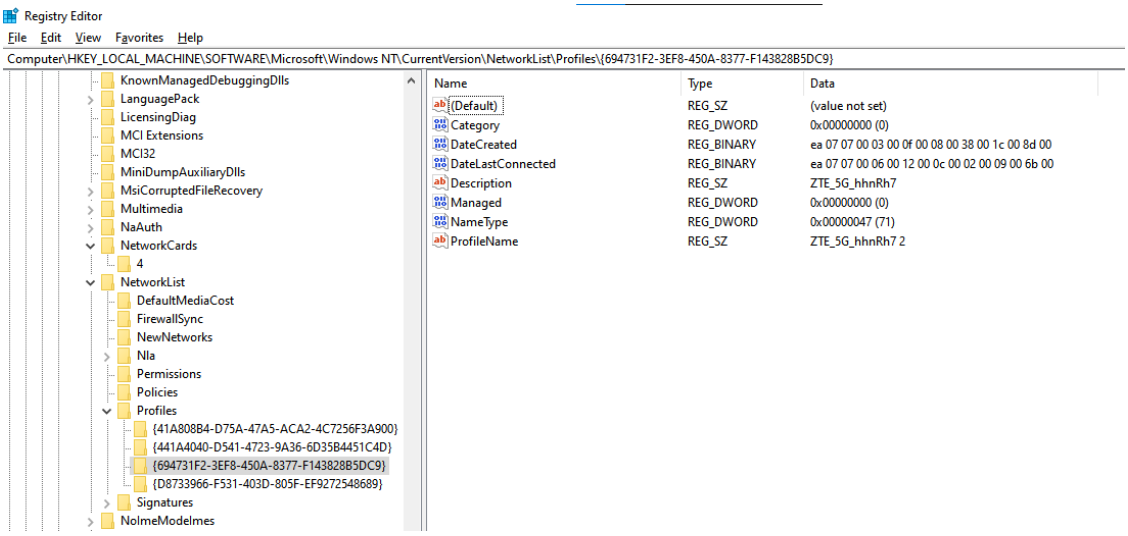


Figure 41. NetworkList profile keys on the host system.

EVIDENCE NOTE: FORENSIC SIGNIFICANCE

> A saved SSID places the machine, at some point, within range of a specific network, which is useful for corroborating a suspect's claimed location or identifying a shared/public network relevant to the case timeline.

Finding 13, Three Removable Storage Devices (Last-Write, Serial, Drive Letter)

Purpose: Examines three specific removable storage devices in detail (connection time, serial number, and drive letter) to assess their potential role in moving files off the system.

Source 1: Autopsy

Registry path: `SYSTEM\ControlSet001\Enum\USBSTOR`

Result: Apple iPod (S/N 00082700148302AB), TREK TD2SMART_G3 (Rev 2.20/2.40), and USB_2.0_Prod_Flash_Disk (Rev 1100), all three parent keys carry the identical LastWrite timestamp of 2007-07-14 17:56:41Z.

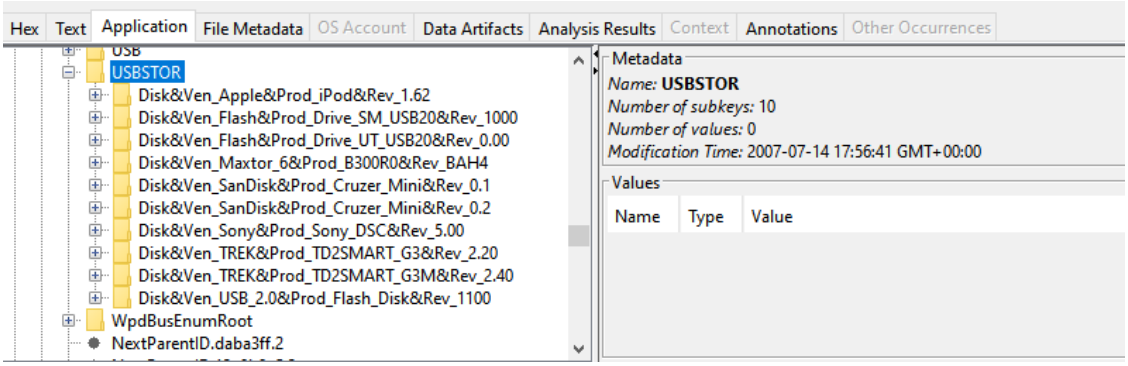


Figure 42. USBSTOR entries for the three removable devices in Autopsy.

Source 2: RegRipper (SYSTEM hive)

Result: Same three devices independently confirmed, alongside a Maxtor 6 B300R0 external drive and a SanDisk Cruzer Mini.

```
usbstor v.20200515
(System) Get USBStor key info

USBStor
ControlSet001\Enum\USBStor

Disk&Ven_Apple&Prod_iPod&Rev_1.62 [2007-07-14 17:56:41]
  S/N: 000A270014B302AB&0 [2007-07-14 17:56:41Z]
  Device Parameters LastWrite: [2007-07-14 17:56:41Z]
  LogConf LastWrite          : [2007-07-14 17:56:41Z]
  Properties LastWrite       : [2007-07-14 17:56:41Z]
    FriendlyName          : Apple iPod USB Device

Disk&Ven_Flash&Prod_Drive_SM_USB20&Rev_1000 [2007-07-14 17:56:41]
  S/N: 6&6b8c30&0&AA14012714842&0 [2007-07-14 17:56:41Z]
  Device Parameters LastWrite: [2007-07-14 17:56:41Z]
  LogConf LastWrite          : [2007-07-14 17:56:41Z]
  Properties LastWrite       : [2007-07-14 17:56:41Z]
    FriendlyName          : Flash Drive SM_USB20 USB Device
  S/N: AA14012714842&0 [2007-07-14 17:56:41Z]
  Device Parameters LastWrite: [2007-07-14 17:56:41Z]
  LogConf LastWrite          : [2007-07-14 17:56:41Z]
  Properties LastWrite       : [2007-07-14 17:56:41Z]
    FriendlyName          : Flash Drive SM_USB20 USB Device

Disk&Ven_Flash&Prod_Drive_UT_USB20&Rev_0.00 [2007-07-14 17:56:41]
  S/N: 0000000000C80F&0 [2007-07-14 17:56:41Z]
  Device Parameters LastWrite: [2007-07-14 17:56:41Z]
  LogConf LastWrite          : [2007-07-14 17:56:41Z]
  Properties LastWrite       : [2007-07-14 17:56:41Z]
    FriendlyName          : Flash Drive UT_USB20 USB Device
  S/N: 0000000000C9BA&0 [2007-07-14 17:56:41Z]
  Device Parameters LastWrite: [2007-07-14 17:56:41Z]
  LogConf LastWrite          : [2007-07-14 17:56:41Z]
  Properties LastWrite       : [2007-07-14 17:56:41Z]
    FriendlyName          : Flash Drive UT_USB20 USB Device

Disk&Ven_Maxtor_6&Prod_B300R0&Rev_BAH4 [2007-07-14 17:56:41]
  S/N: 8396 [2007-07-14 17:56:41Z]
  Device Parameters LastWrite: [2007-07-14 17:56:41Z]
  LogConf LastWrite          : [2007-07-14 17:56:41Z]
  Properties LastWrite       : [2007-07-14 17:56:41Z]
    FriendlyName          : Maxtor 6 B300R0 USB Device
```

Figure 43. usbstor plugin output listing the removable devices.

Source 3: Host Registry Comparison

Result: USBSTOR key structure (General UDisk / Generic Mass-Storage / MXT-USB Storage Device) confirmed on the host for comparison.

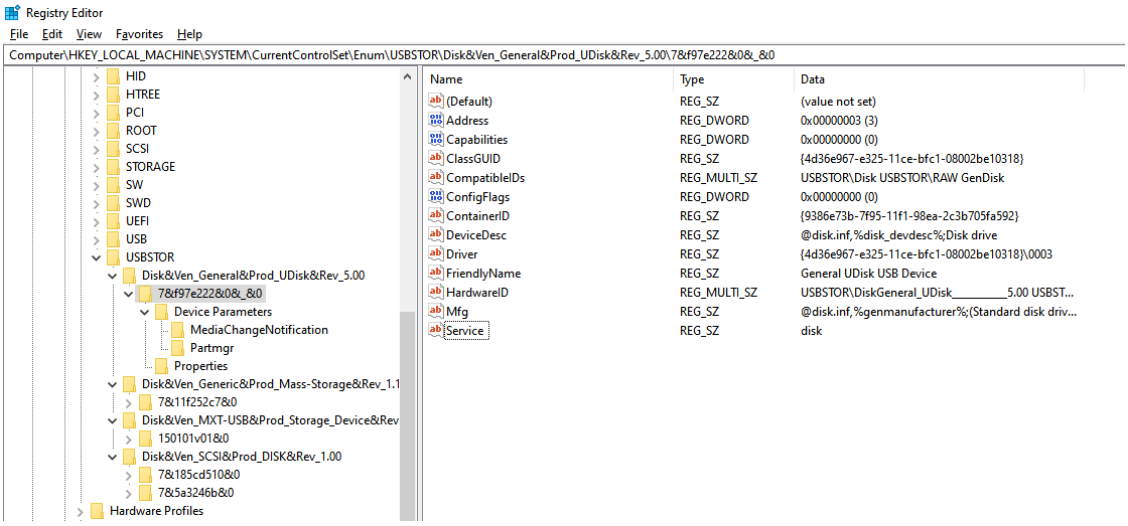


Figure 44. USBSTOR entries on the host comparison system.

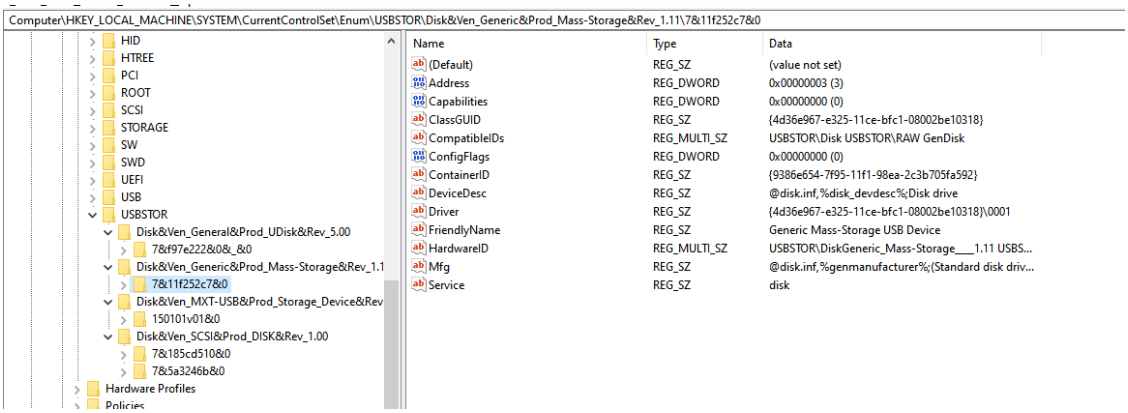


Figure 45. USBSTOR entries on the host comparison system.

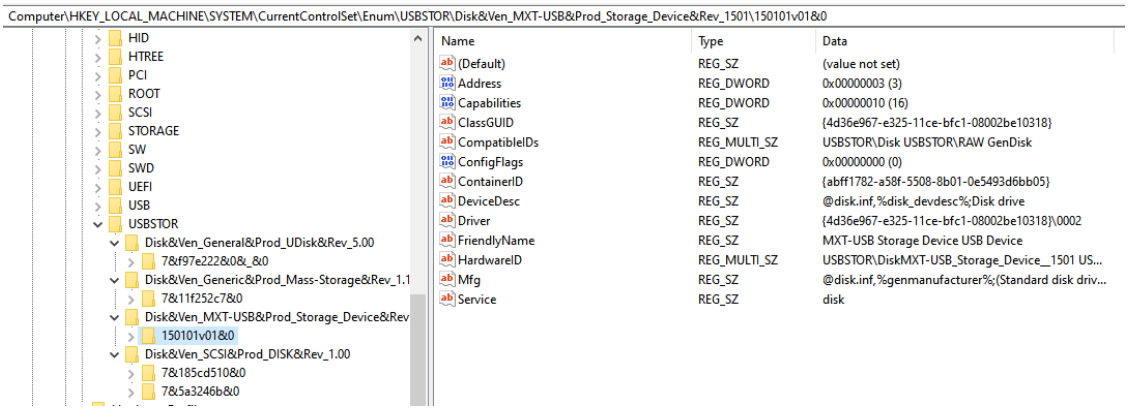


Figure 46. USBSTOR entries on the host comparison system.

EVIDENCE NOTE: FORENSIC SIGNIFICANCE

All three devices sharing an identical LastWrite time is expected behavior, not a coincidence: LastWrite on the parent USBSTOR key updates only on first-ever connection, so devices first plugged in during the same session legitimately share a timestamp.

The mix of an Apple iPod (audio/media capacity) and flash-type drives is worth noting given the media-player and Recent Documents artifacts found elsewhere (Findings 27 and 30), all are plausible vehicles for moving files off the system.

Finding 14, Five Installed Software Titles (with Install Timestamps)

Purpose: Builds a timeline of software installation on the system, to identify when key tools (including encryption utilities) were introduced.

Source 1: Autopsy

Registry path: `SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall`

Result: AOL Uninstaller (2007-02-27 20:57:42Z); AIM_6 (2007-02-27 19:21:04Z); ActiveTouchMeetingClient / WebEx (2007-10-10 10:12:40Z); BestCrypt 8.0 (2007-02-27 23:08:21Z); FileZilla (2007-06-24 00:23:53Z).

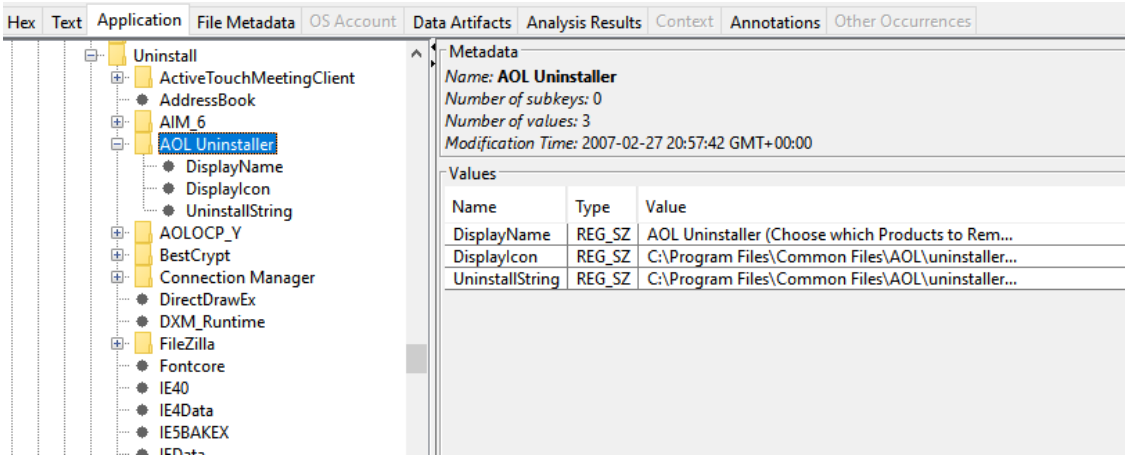


Figure 47. Installed-application registry entries browsed in Autopsy, including BestCrypt and Mozilla Firefox.

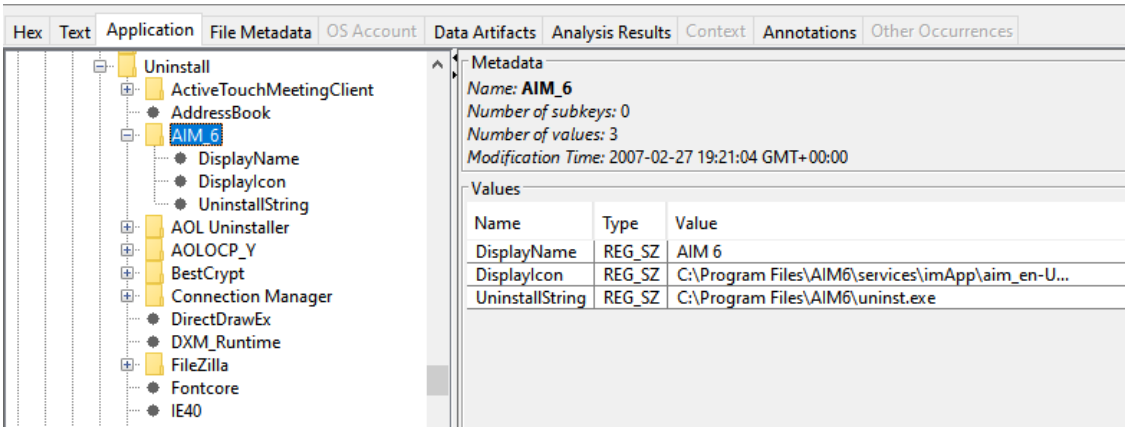


Figure 48. Installed-application registry entries browsed in Autopsy, including BestCrypt and Mozilla Firefox.

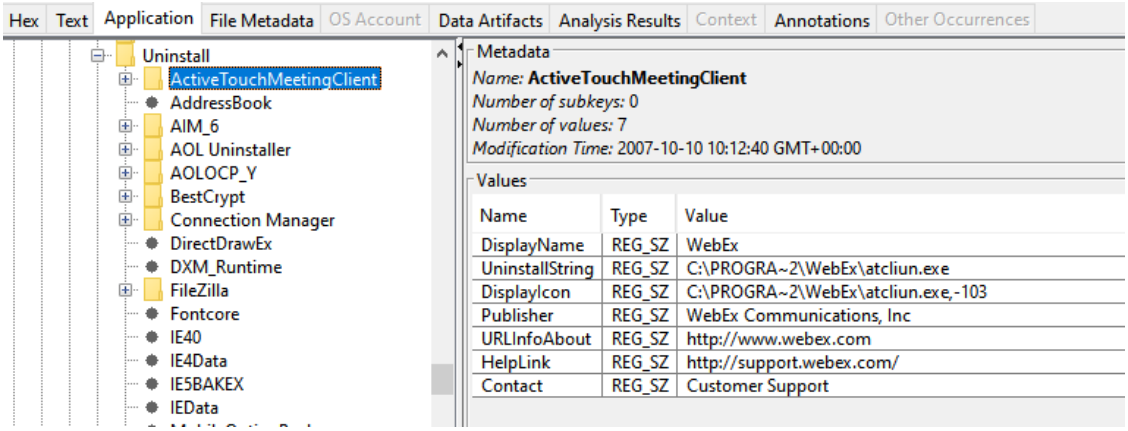


Figure 49. Installed-application registry entries browsed in Autopsy, including BestCrypt and Mozilla Firefox.

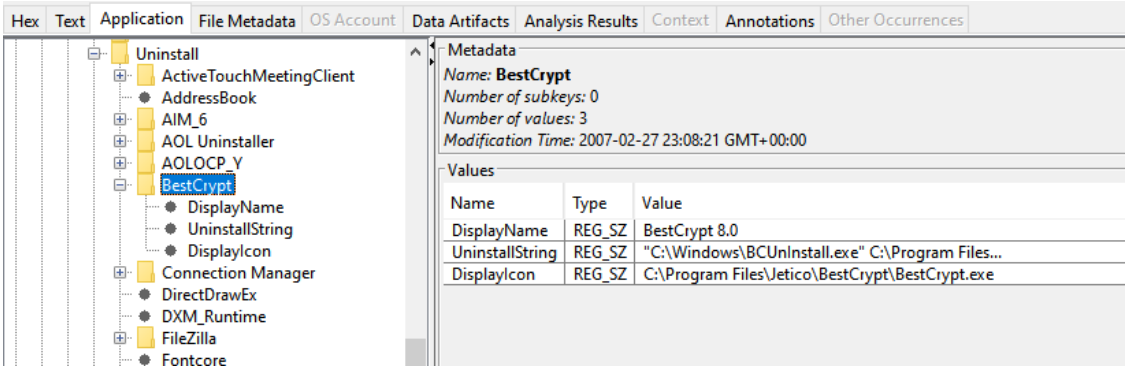


Figure 50. Installed-application registry entries browsed in Autopsy, including BestCrypt and Mozilla Firefox.

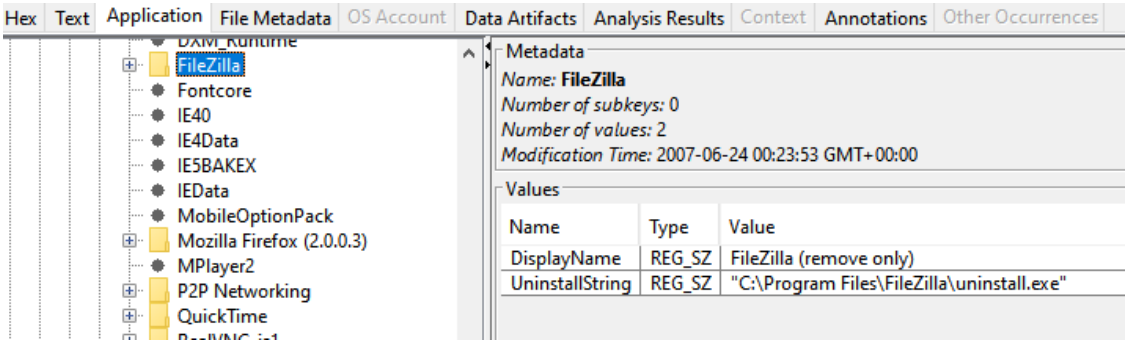


Figure 51. Installed-application registry entries browsed in Autopsy, including BestCrypt and Mozilla Firefox.

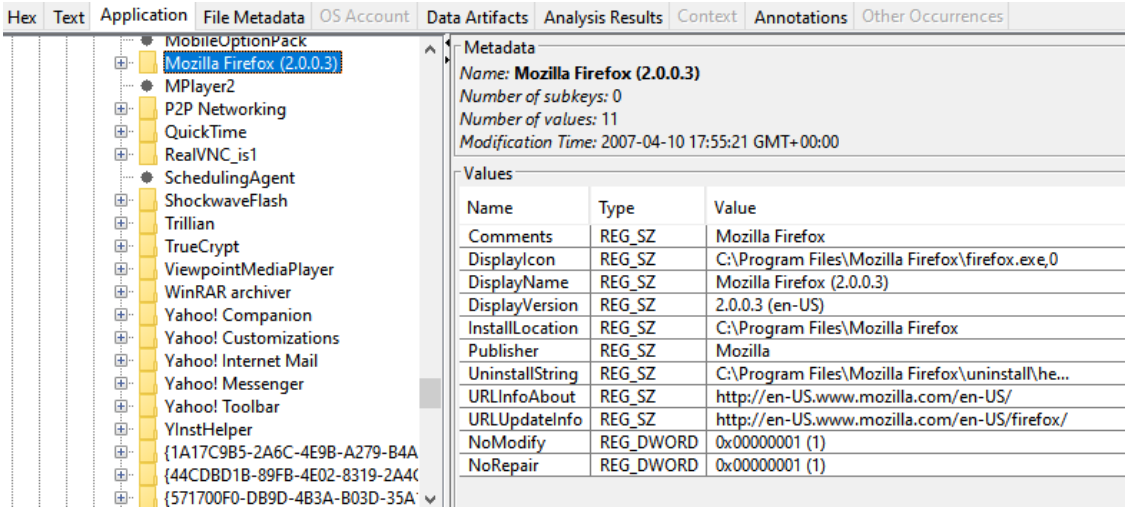


Figure 52. Installed-application registry entries browsed in Autopsy, including BestCrypt and Mozilla Firefox.

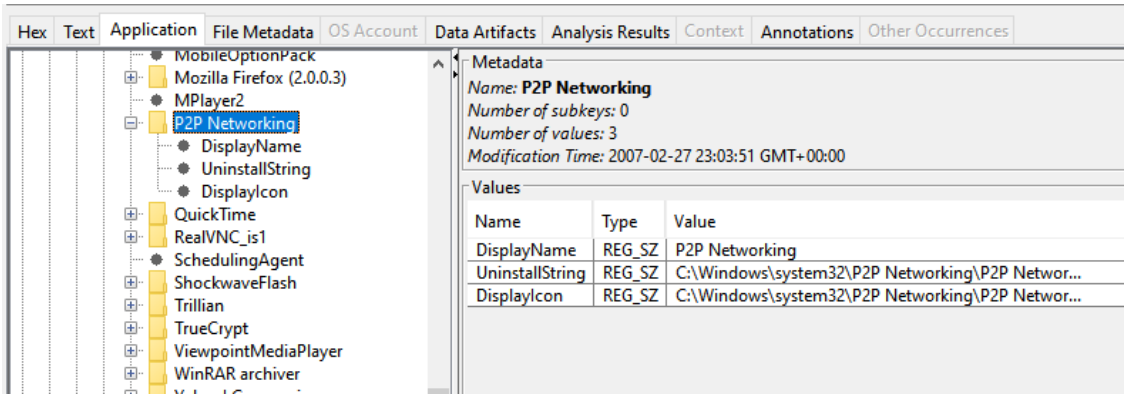


Figure 53. Installed-application registry entries browsed in Autopsy, including BestCrypt and Mozilla Firefox.

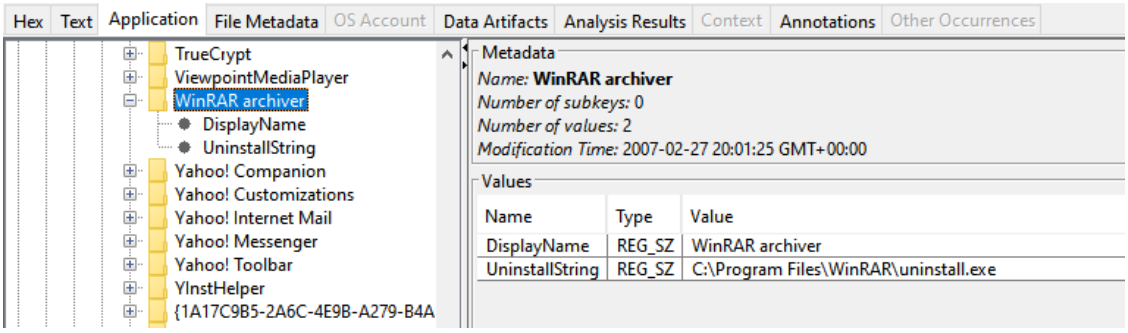


Figure 54. Installed-application registry entries browsed in Autopsy, including BestCrypt and Mozilla Firefox.

Source 2: RegRipper (SOFTWARE hive)

Result: uninstall plugin corroborates the list and adds: TrueCrypt (2007-04-10 17:55:21Z), VNC Free Edition 4.1.2 (2007-04-11 01:37:31Z), Adobe Reader 8 (2007-04-11 17:24:00Z), AccessData Registry Viewer 1.5, and Microsoft Office Standard 2003.

```
Uninstall
Microsoft\Windows\CurrentVersion\Uninstall

2007-10-10 10:12:40Z
  WebEx

2007-06-24 00:23:53Z
  FileZilla (remove only)

2007-04-17 23:25:28Z
  Microsoft Office Standard Edition 2003 v.11.0.5614.0

2007-04-17 21:43:27Z
  RTC Client API v1.2 v.1.2.0000

2007-04-17 19:58:46Z
  AccessData DNA 3 Worker v.3.3

2007-04-14 00:01:22Z
  AccessData Registry Viewer v.1.5

2007-04-13 23:36:51Z
  QuickTime

2007-04-12 23:26:59Z
  Adobe Reader 8 v.8.0.0

2007-04-11 17:24:00Z
  VNC Free Edition 4.1.2 v.4.1.2

2007-04-11 01:37:31Z
  TrueCrypt

2007-04-10 17:55:21Z
  Mozilla Firefox (2.0.0.3) v.2.0.0.3 (en-US)
```

Figure 55. uninstall plugin output listing installed applications chronologically.

Source 3: Host Registry Comparison

Result: Equivalent Uninstall key entries confirmed on the host (e.g. CodeMeter Runtime Kit, Exterro FTK Imager, Autopsy itself, Windows Update Health Tools).

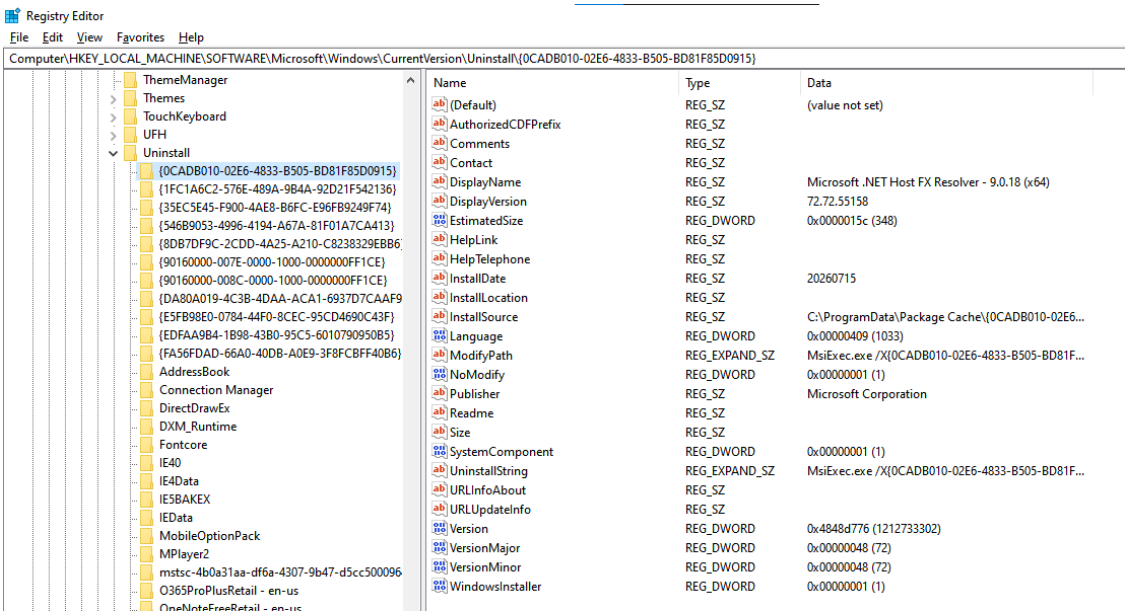


Figure 56. Installed applications on the host comparison system.

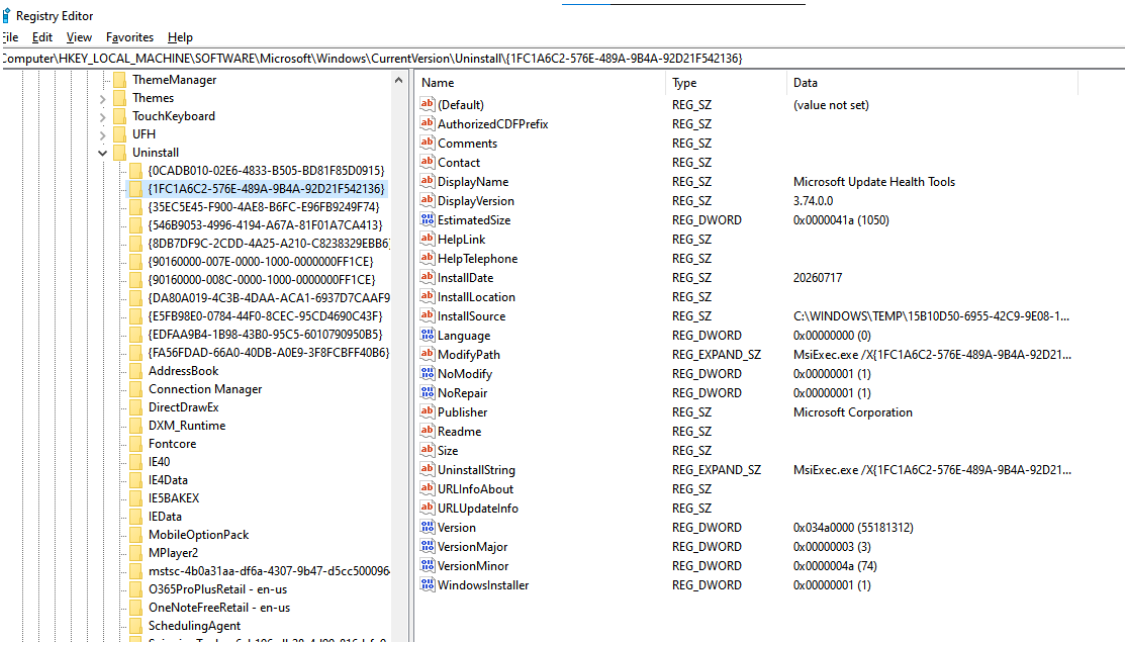


Figure 57. Installed applications on the host comparison system.

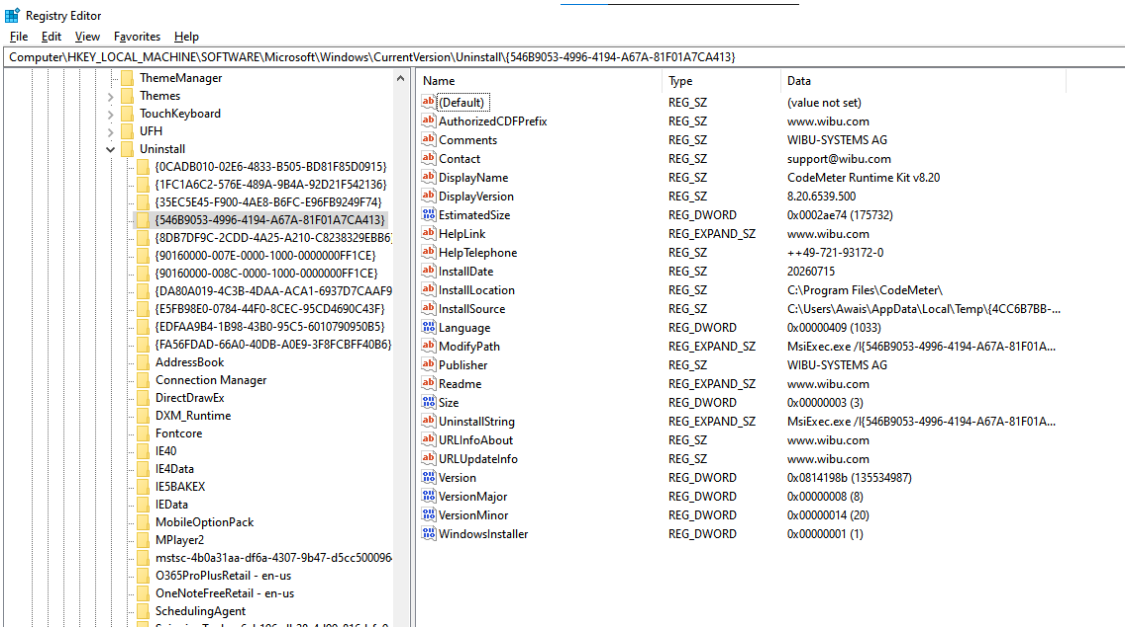


Figure 58. Installed applications on the host comparison system.

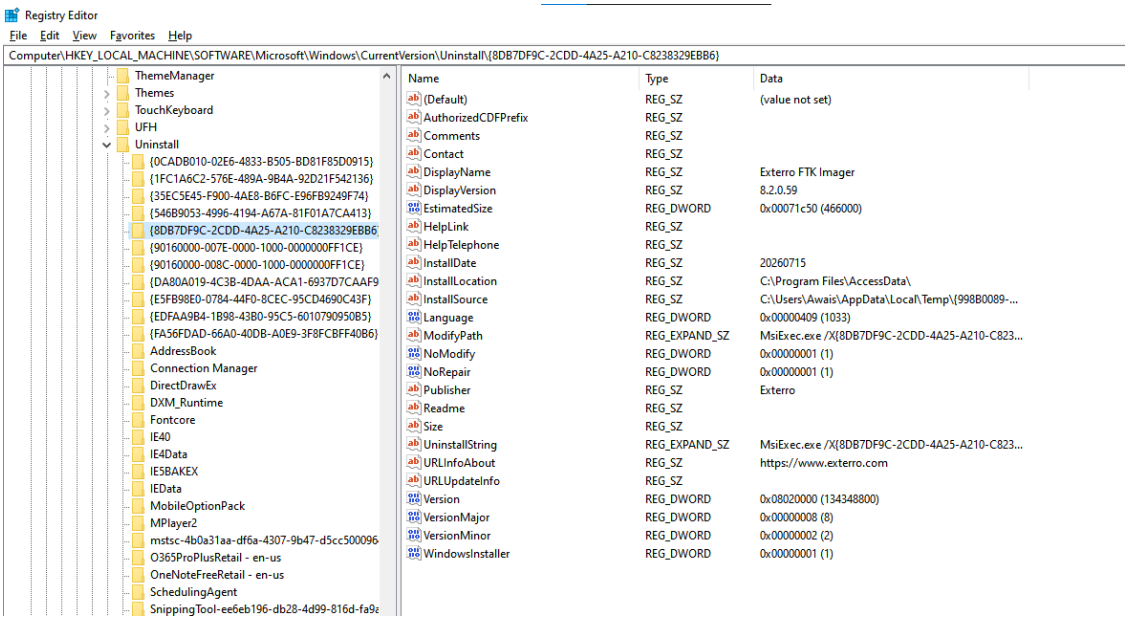


Figure 59. Installed applications on the host comparison system.

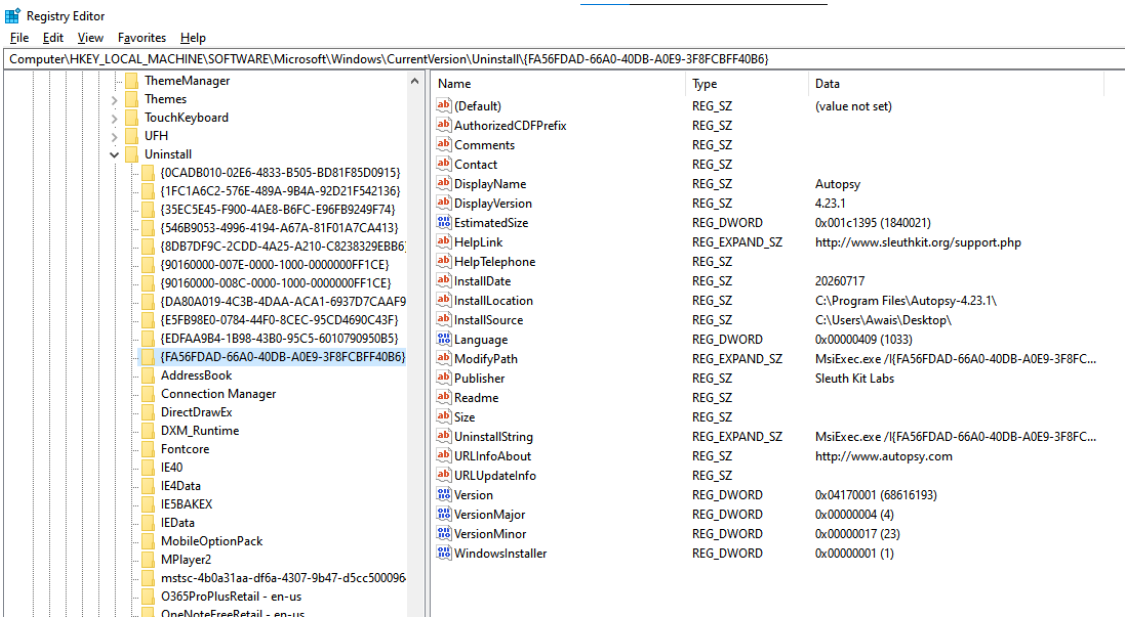


Figure 60. Installed applications on the host comparison system.

Finding 15, Registered Organization, Install Date, Product ID, Product Name, Registered Owner

Purpose: Confirms the licensing/registration details of the operating system itself, tying the machine to a specific registered owner and organization.

Source 1: Autopsy

Registry path: `SOFTWARE\Microsoft\Windows NT\CurrentVersion`

Result: ProductName: Windows Vista (TM) Ultimate; RegisteredOwner: Wes Mantooth; RegisteredOrganization: Volturi Enterprises; ProductId: 89580-378-0753292-71704.

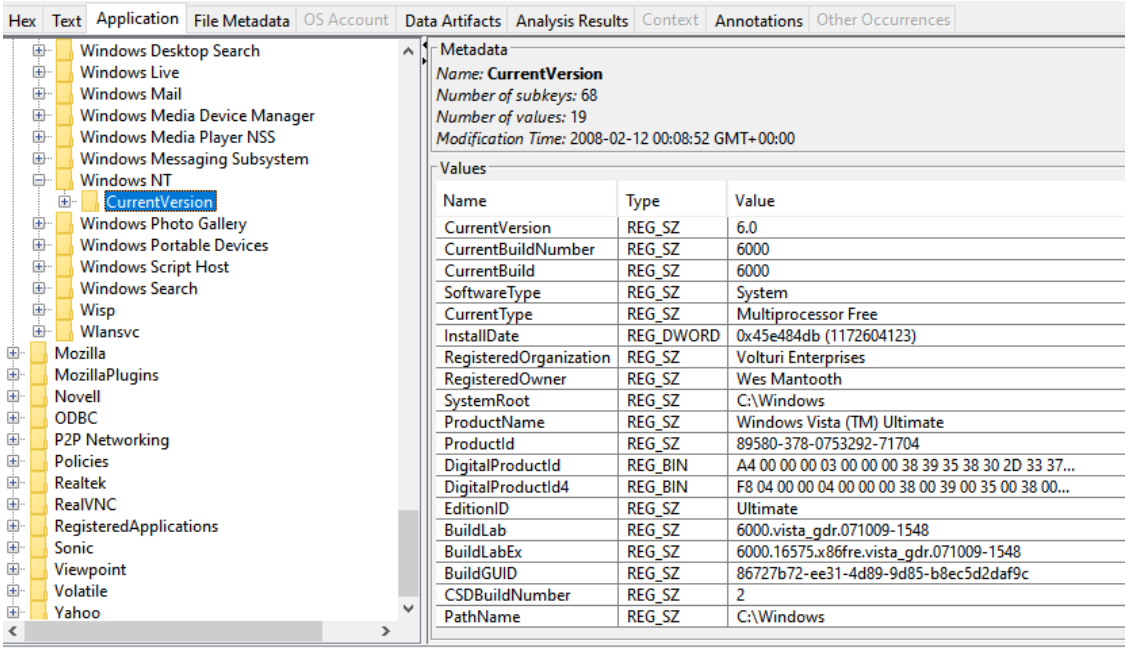


Figure 61. CurrentVersion registration block in Autopsy.

Source 2: RegRipper (SOFTWARE hive)

Result: winver plugin confirms: BuildLab 6000.vista_gdr.071009-1548; InstallDate 2007-02-27 19:22:03Z.

```
winver v.20200525
(Software) Get Windows version & build info

ProductName                Windows Vista (TM) Ultimate
BuildLab                   6000.vista_gdr.071009-1548
BuildLabEx                 6000.16575.x86fre.vista_gdr.071009-1548
RegisteredOrganization     Volturi Enterprises
RegisteredOwner            Wes Mantooth
InstallDate                2007-02-27 19:22:03Z
```

Figure 62. winver plugin output.

Source 3: Host Registry Comparison

Result: Host system: ProductName Windows 10 Home; illustrates the same CurrentVersion key persisted through later Windows versions.

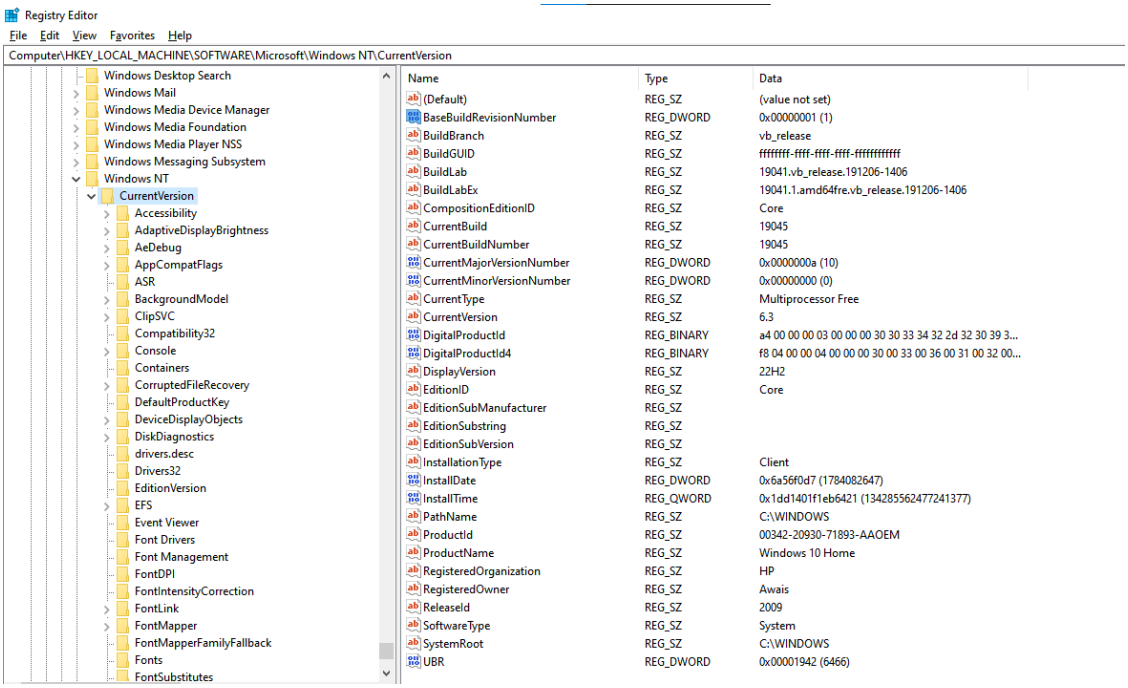


Figure 63. CurrentVersion key on the host comparison system.

Finding 16, User Profiles Present on the System

Purpose: Enumerates every local user profile on the system, establishing which accounts existed before investigating their individual activity.

Source 1: Autopsy

Registry path: `SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList`

Result: Wes Mantooth, C:\Users\Wes Mantooth (SID ...-1000); Dracula, C:\Users\Dracula (SID ...-1002); plus built-in System/LocalService/NetworkService profiles.

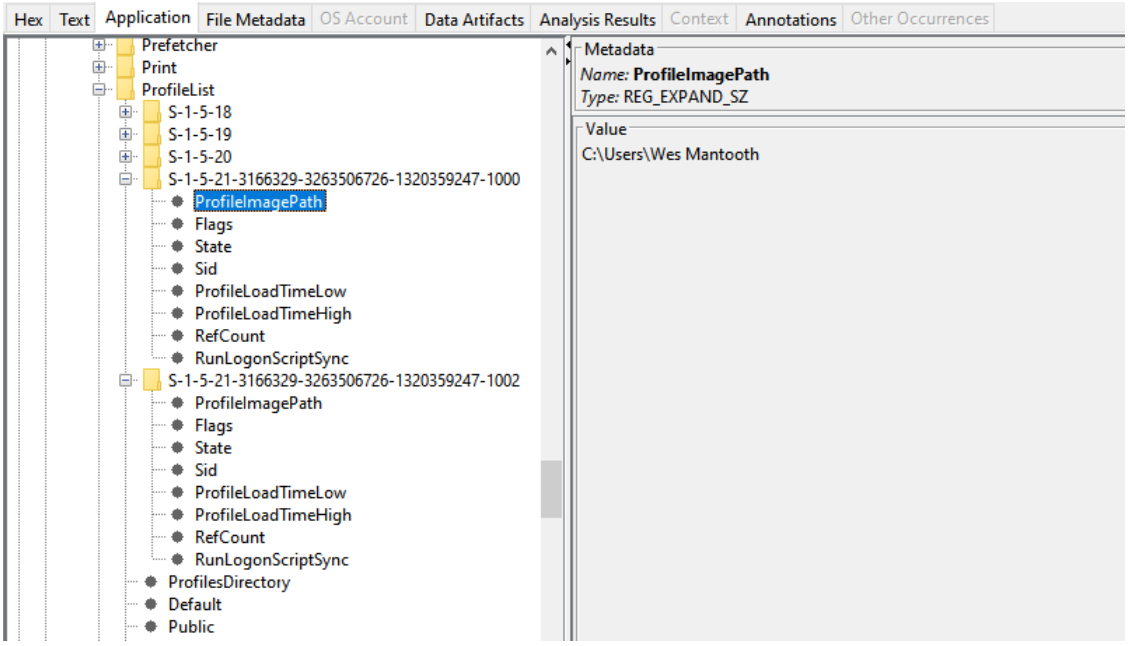


Figure 64. ProfileList entries in Autopsy for Wes Mantooth and Dracula.

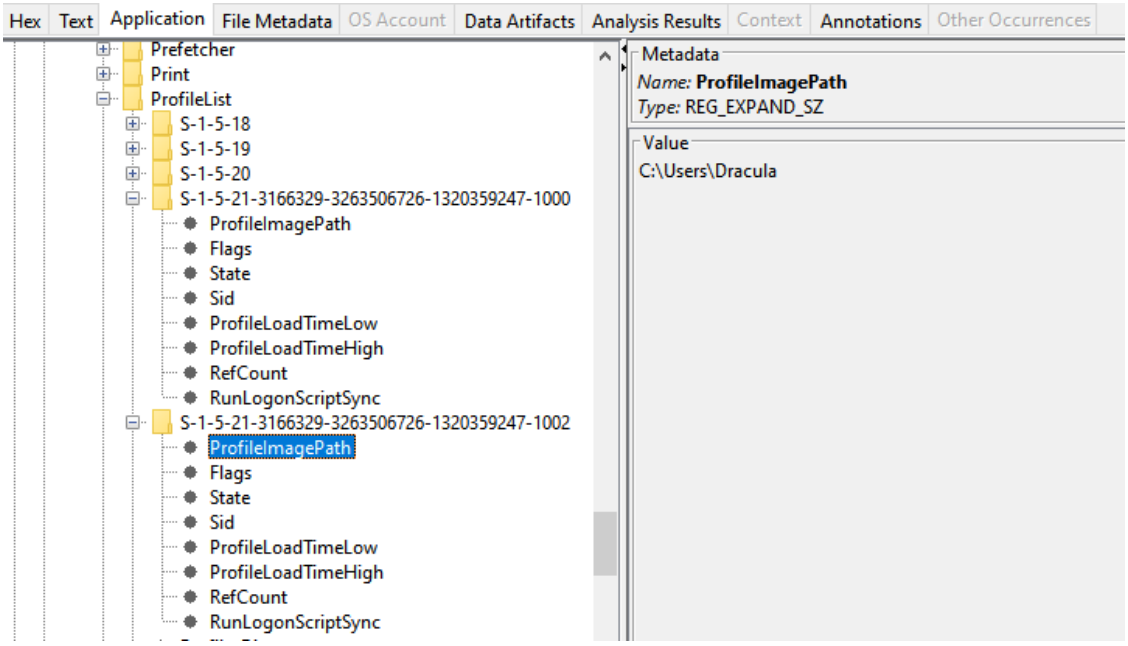


Figure 65. ProfileList entries in Autopsy for Wes Mantooth and Dracula.

Source 2: RegRipper (SOFTWARE hive)

Result: profilelist plugin confirms both paths and SIDs, with LastWrite 2008-02-12 20:13:25Z (Wes Mantooth) and 2007-03-23 (Dracula).

```
profilelist v.20200518
(Software) Get content of ProfileList key

Microsoft\Windows NT\CurrentVersion\ProfileList

Path      : %systemroot%\system32\config\systemprofile
SID       : S-1-5-18
LastWrite : 2006-11-02 12:51:44Z

Path      : %SystemRoot%\ServiceProfiles\LocalService
SID       : S-1-5-19
LastWrite : 2006-11-02 12:51:44Z

Path      : %SystemRoot%\ServiceProfiles\NetworkService
SID       : S-1-5-20
LastWrite : 2006-11-02 12:51:44Z

Path      : C:\Users\Wes Mantooth
SID       : S-1-5-21-3166329-3263506726-1320359247-1000
LastWrite : 2008-02-12 20:13:25Z

Path      : C:\Users\Dracula
SID       : S-1-5-21-3166329-3263506726-1320359247-1002
LastWrite : 2007-03-23 00:31:49Z
```

Figure 66. profilelist plugin output.

Source 3: Host Registry Comparison

Result: Host profile (C:\Users\Awais) located under the same ProfileList structure.

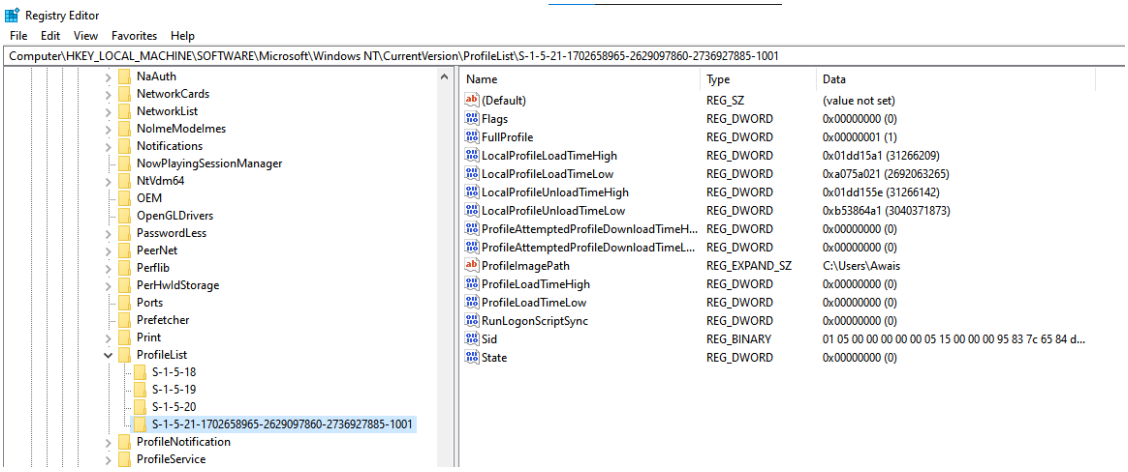


Figure 67. ProfileList key on the host comparison system.

Finding 17, SAM Account Details Per User (Login Count, Last Login, Failed Logins)

Purpose: Extracts detailed account-level statistics (login counts, last login, failed logins) for each user, to identify which accounts were actually in active use.

Source 1: Autopsy

Registry path: `SAM\SAM\Domains\Account\Users\<RID>`

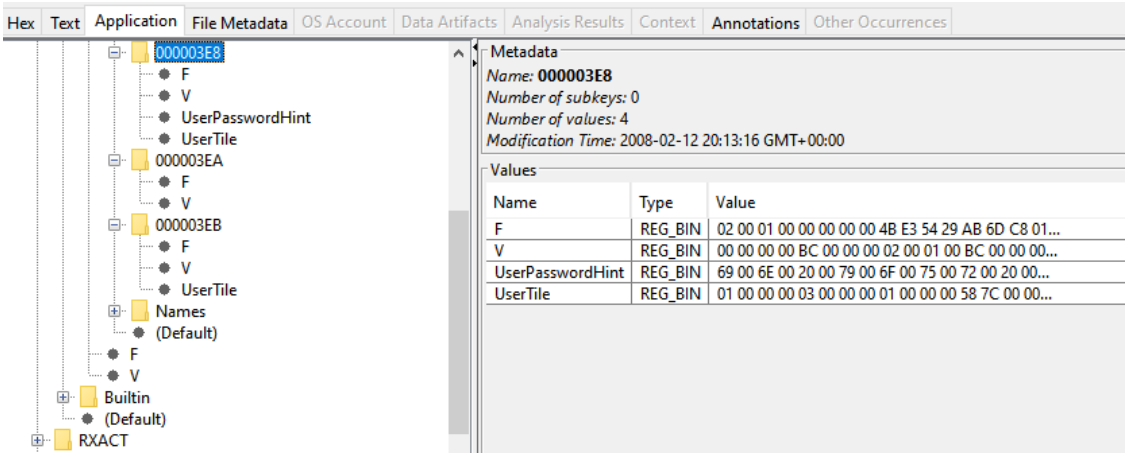


Figure 68. Raw V-value structure for a SAM user record, viewed in Autopsy's hex view.

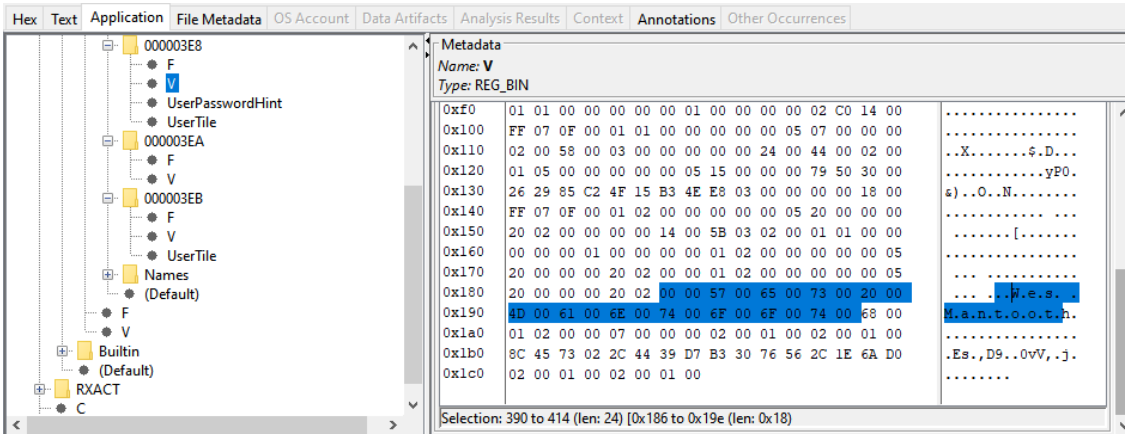


Figure 69. Raw V-value structure for a SAM user record, viewed in Autopsy's hex view.

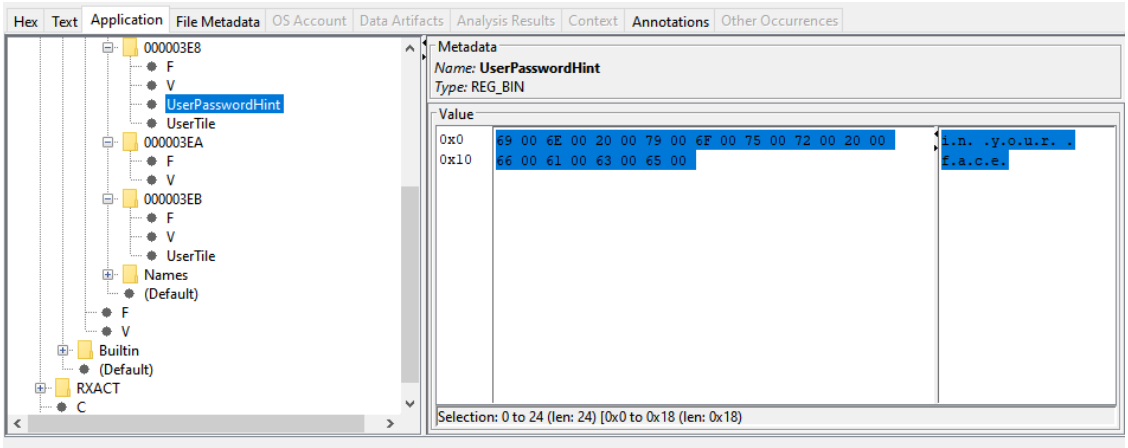


Figure 70. Raw V-value structure for a SAM user record, viewed in Autopsy's hex view.

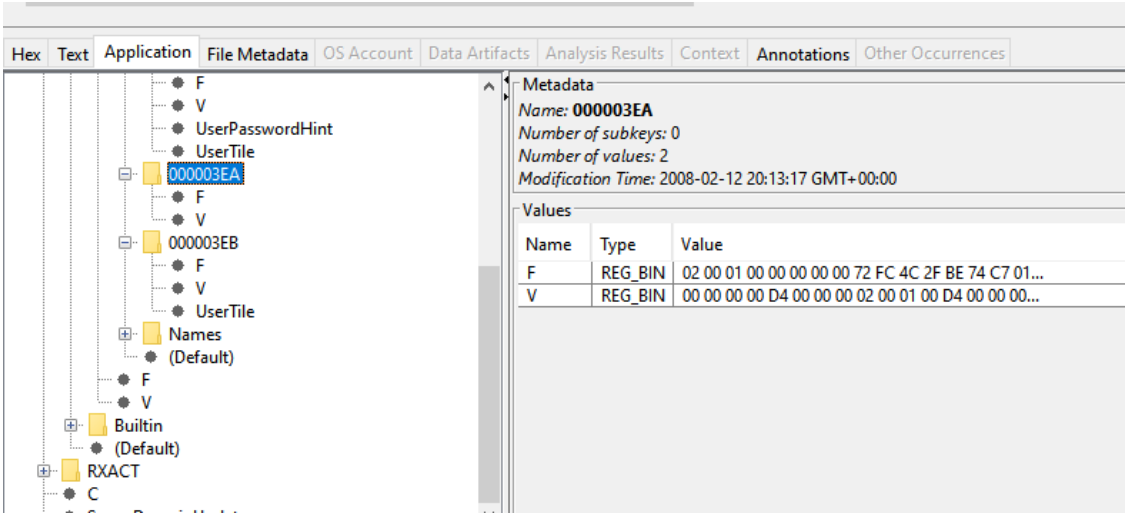


Figure 71. Raw V-value structure for a second SAM user record.

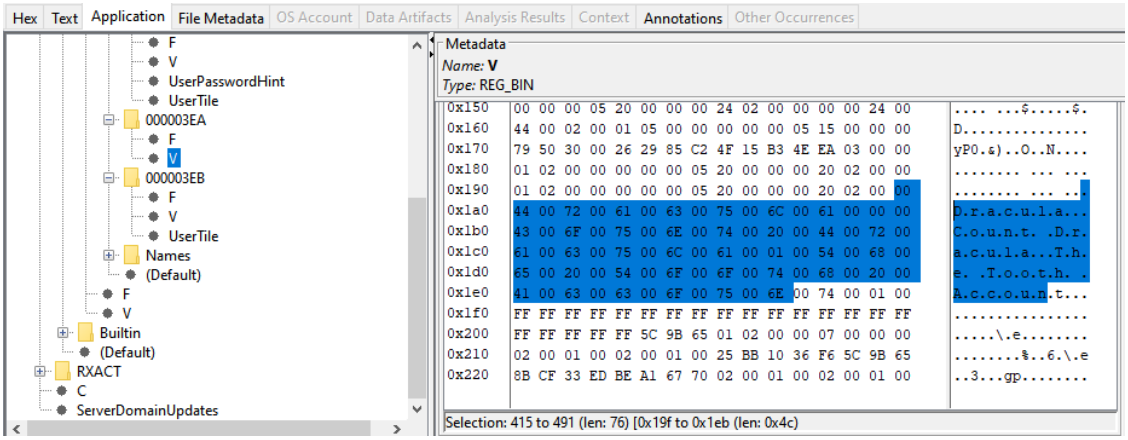


Figure 72. Raw V-value structure for a second SAM user record.

Source 2: RegRipper (SAM hive)

Result: Administrator [500]: Disabled, Login Count 0. Guest [501]: Disabled, Login Count 0.

```
User Information
------------------------
Username        : Administrator [500]
SID             : S-1-5-21-3166329-3263506726-1320359247-500
Full Name       :
User Comment    : Built-in account for administering the computer/domain
Account Type    : Default Admin User
Account Created : Tue Feb 27 18:29:26 2007 Z
Name            :
Last Login Date : Thu Nov  2 13:02:01 2006 Z
Pwd Reset Date  : Thu Nov  2 13:08:15 2006 Z
Pwd Fail Date   : Never
Login Count     : 1
  --> Password does not expire
  --> Account Disabled
  --> Normal user account

Username        : Guest [501]
SID             : S-1-5-21-3166329-3263506726-1320359247-501
Full Name       :
User Comment    : Built-in account for guest access to the computer/domain
Account Type    : Default Guest Acct
Account Created : Tue Feb 27 18:29:26 2007 Z
Name            :
Last Login Date : Never
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Login Count     : 0
  --> Password does not expire
  --> Account Disabled
  --> Password not required
  --> Normal user account
```

Figure 73. samparse plugin output for the Administrator and Guest accounts.

Result: Wes Mantooth [1000]: Admin account, Password Hint “in your face”, Last Login 2008-02-12 19:12:08Z, Pwd Fail Date 2008-02-12 20:13:16Z, Login Count 96. Dracula [1002]: Full Name “Count Dracula”, Custom Limited Acct, Last Login 2007-04-02 00:30:58Z, Pwd Fail Date 2008-02-12 20:13:17Z, Login Count 3.

```
Username        : Wes Mantooth [1000]
SID             : S-1-5-21-3166329-3263506726-1320359247-1000
Full Name       :
User Comment    :
Account Type    : Default Admin User
Account Created : Tue Feb 27 18:29:10 2007 Z
Name            :
Password Hint   : in your face
Last Login Date : Tue Feb 12 19:12:08 2008 Z
Pwd Reset Date  : Tue Feb 27 18:29:13 2007 Z
Pwd Fail Date   : Tue Feb 12 20:13:16 2008 Z
Login Count     : 96
  --> Password does not expire
  --> Password not required
  --> Normal user account

Username        : Dracula [1002]
SID             : S-1-5-21-3166329-3263506726-1320359247-1002
Full Name       : Count Dracula
User Comment    : The Tooth Account
Account Type    : Custom Limited Acct
Account Created : Tue Mar  6 01:25:43 2007 Z
Name            :
Last Login Date : Mon Apr  2 00:30:58 2007 Z
Pwd Reset Date  : Mon Apr  2 00:30:39 2007 Z
Pwd Fail Date   : Tue Feb 12 20:13:17 2008 Z
Login Count     : 3
  --> Password does not expire
  --> Normal user account
```

Figure 74. samparse plugin output for Wes Mantooth and Dracula.

Result: Laurent [1003]: Custom Limited Acct, created 2008-02-12, never logged in.

```
Username        : Laurent [1003]
SID             : S-1-5-21-3166329-3263506726-1320359247-1003
Full Name       : Laurent
User Comment    :
Account Type    : Custom Limited Acct
Account Created : Tue Feb 12 00:13:36 2008 Z
Name            :
Last Login Date : Never
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Login Count     : 0
  --> Password does not expire
  --> Normal user account
```

Figure 75. samparse plugin output for the Laurent account.

Source 3: Host Registry Comparison

Result: SAM\Domains\Account\Users structure confirmed on the host for comparison (account details not disclosed).

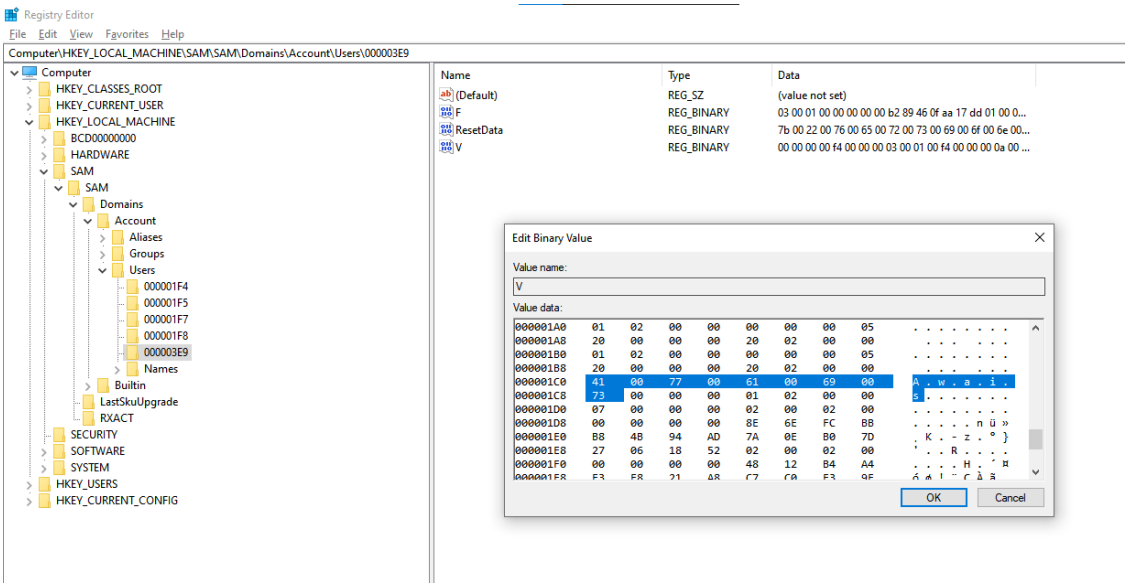


Figure 76. SAM Users key on the host comparison system.

Finding 18, Which User Account Warrants Further Investigation, and Why

Purpose: Synthesizes the account data from Finding 17 into an investigative judgment about which account(s) most warrant further examination, and why.

Wes Mantooth [RID 1000] is the primary subject: an Admin-level account with 96 recorded logins, a personal password hint ("in your face"), and a profile that is the source of every case-relevant file artifact in this examination (Findings 19–35).

Dracula [RID 1002] is the secondary account of interest. Its SAM record shows a failed-login timestamp of 2008-02-12 20:13:17Z, exactly one second after Wes Mantooth's own failed-login timestamp of 2008-02-12 20:13:16Z. That one-second gap is tight enough to warrant explanation: it is consistent with either the same physical person attempting both accounts in quick succession, or a scripted/automated logon attempt, and should not be dismissed as coincidental without further timeline correlation against Security Event Log logon events (Event ID 4624/4625).

Administrator [500] and Guest [501] are both disabled with zero recorded logins and are dismissed as lower priority. Laurent [1003] was created 2008-02-12 (the same day as the Dracula/Wes Mantooth failed-login events) but has never been logged into, its creation on that specific date is worth noting as a possible artifact of the same session, even though the account itself shows no activity.

Finding 19, Recent PDF Files Opened by Wes Mantooth

Purpose: Recovers the specific PDF files the primary user account recently opened, to identify documents worth reviewing in full.

Source 1: Autopsy

Registry path:
`NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.pdf`

Result: order851797-2007-04-12-13-17-02.pdf and order851797-2007-04-12-13-17-02 (1).pdf, an online order confirmation, opened twice.

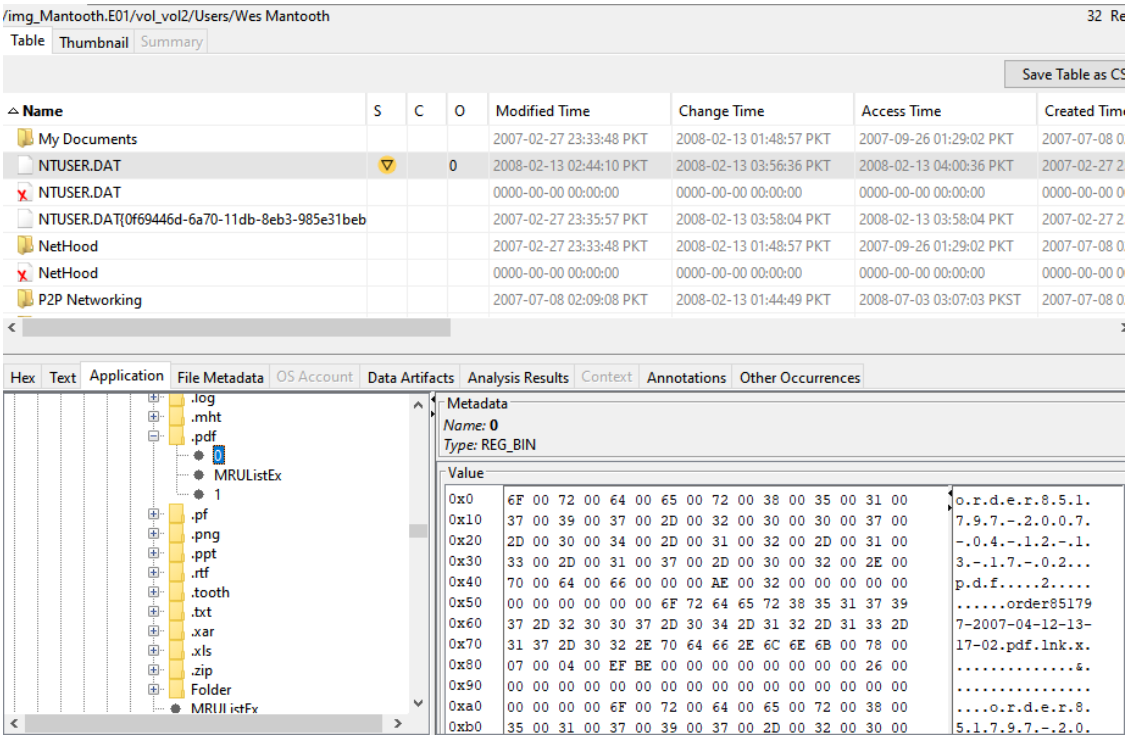


Figure 77. RecentDocs\.pdf MRU list and raw MRUListEx bytes for Wes Mantooth, in Autopsy.

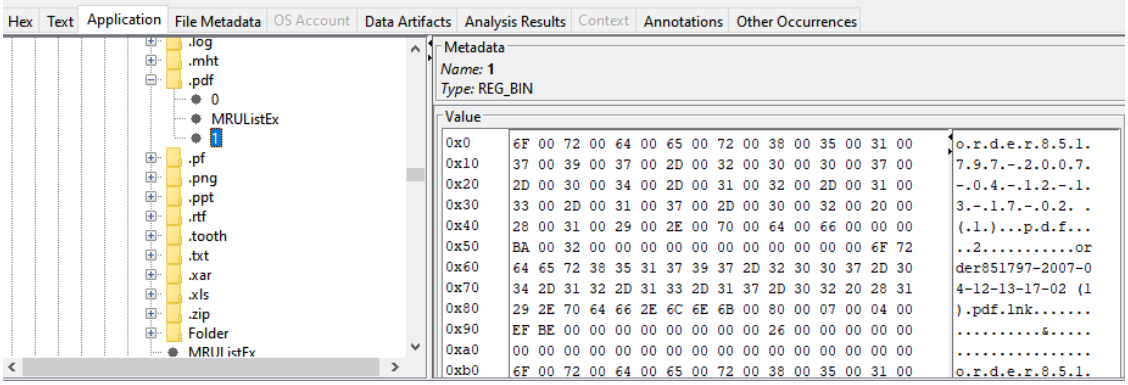


Figure 78. RecentDocs\.pdf MRU list and raw MRUListEx bytes for Wes Mantooth, in Autopsy.

Cross-checked via the ComDlg32\OpenSavePidlMRU\pdf key, which independently confirms the same filename.

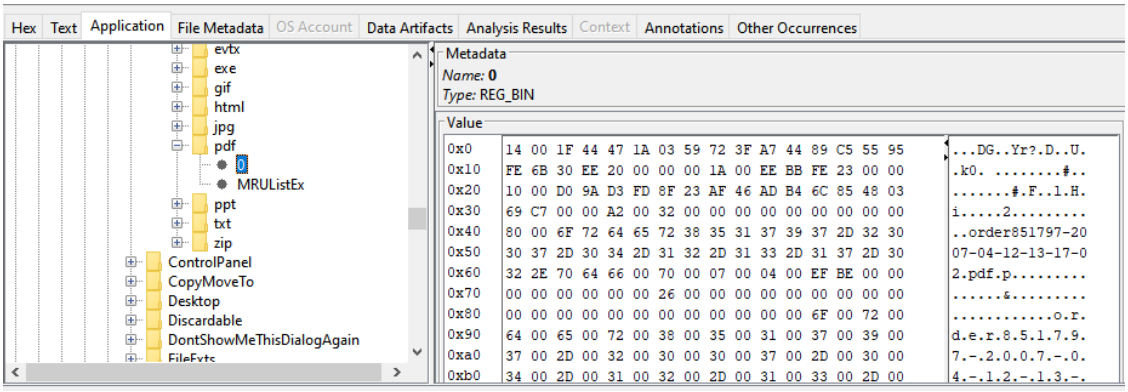


Figure 79. OpenSavePidlMRU\pdf raw MRU bytes confirming the same recent PDF file.

Source 2: RegRipper (NTUSER.DAT)

Result: recentdocs plugin confirms MRUListEx = 1,0 resolving to the same two order851797 PDF filenames, LastWrite 2007-04-13 00:28:47Z.

```
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.pdf
LastWrite Time 2007-04-13 00:28:47Z
MRUListEx = 1,0
  1 = order851797-2007-04-12-13-17-02 (1).pdf
  0 = order851797-2007-04-12-13-17-02.pdf
```

Figure 80. recentdocs plugin output for the .pdf subkey.

Source 3: Host Registry Comparison

Result: RecentDocs key structure located on the host for comparison; no .pdf subkey activity of evidentiary relevance.

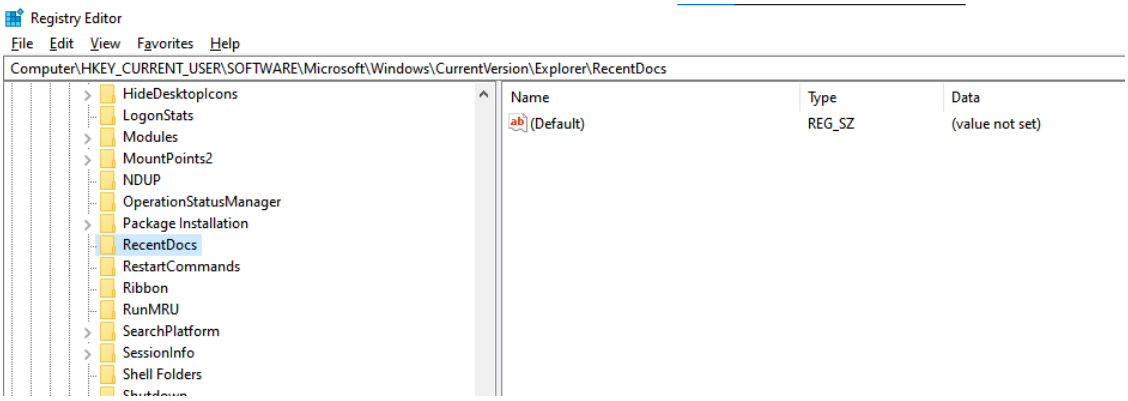


Figure 81. RecentDocs key on the host comparison system.

Finding 20, Three Most Recent Paint Files

Purpose: Recovers the specific image files recently edited in Paint by the primary user account, to identify possible document-editing or forgery activity.

Source 1: Autopsy

Registry path: `NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Applets\Paint\Recent File List`

Result: File1: nationaltall.bmp; File2: prescription.gif; File3: nationaltal.gif; File4: nationaltall.gif, all under C:\Users\Wes Mantooth\Documents\Scripts.

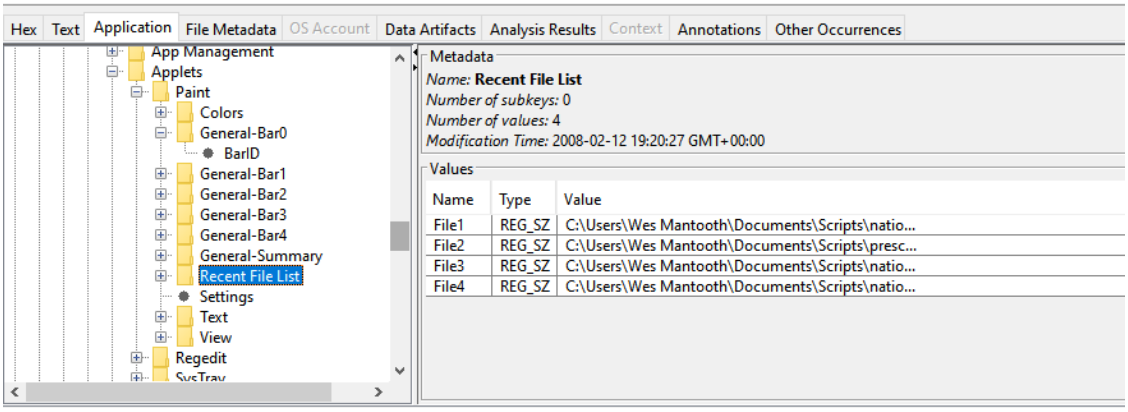


Figure 82. Paint\Recent File List entries in Autopsy.

Source 2: RegRipper (NTUSER.DAT)

Result: applets plugin confirms the same four files, LastWrite 2008-02-12 19:20:27Z, plus a related RegEdit LastKey entry from the same session (19:56:15Z).

```
applets v.20201020
(NTUSER.DAT) Gets contents of user's Applets key
MITRE: T1204 (program execution)

Applets
Software\Microsoft\Windows\CurrentVersion\Applets
LastWrite Time 2007-04-13 00:17:17Z

Software\Microsoft\Windows\CurrentVersion\Applets\Paint\Recent File List
LastWrite Time 2008-02-12 19:20:27Z
  File1 -> C:\Users\Wes Mantooth\Documents\Scripts\nationaltall.bmp
  File2 -> C:\Users\Wes Mantooth\Documents\Scripts\prescription.gif
  File3 -> C:\Users\Wes Mantooth\Documents\Scripts\nationaltal.gif
  File4 -> C:\Users\Wes Mantooth\Documents\Scripts\nationaltall.gif

Software\Microsoft\Windows\CurrentVersion\Applets\Regedit
LastWrite Time 2008-02-12 19:56:15Z
RegEdit LastKey value -> Computer\HKEY_CURRENT_USER
```

Figure 83. applets plugin output listing the Paint Recent File List.

Source 3: Host Registry Comparison

Result: Microsoft Paint has not been executed on the host comparison system, no Recent File List entries exist for this application.

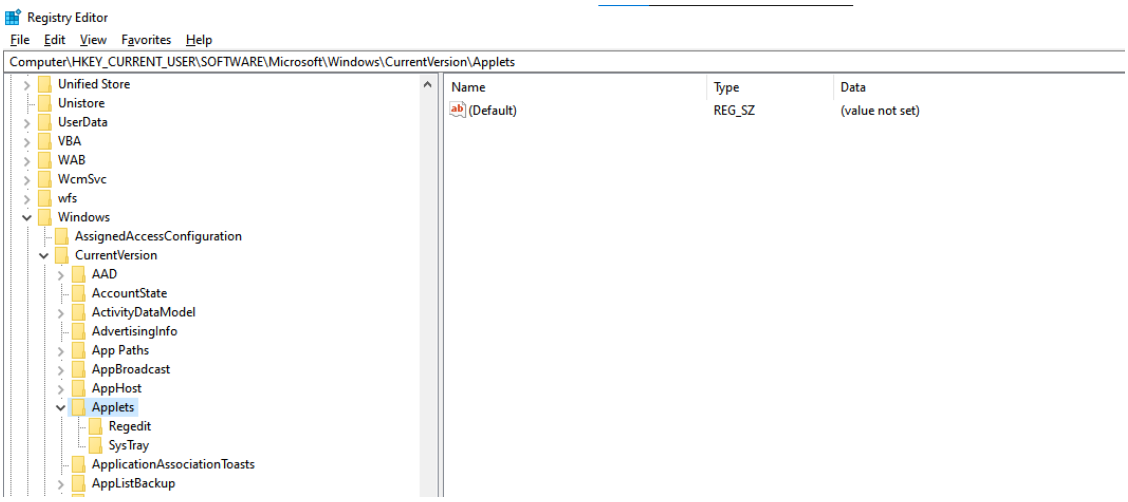


Figure 84. Absent/empty Paint MRU entry on the host comparison system.

> **EVIDENCE NOTE: FORENSIC SIGNIFICANCE**
>
> The filename "prescription.gif" alongside "nationaltall"-named files edited in Paint, combined with "Prescription2.gif" and "doc-prescription.jpg" later found in the broader Recent Documents list (Finding 30), is worth flagging as a possible document-forgery indicator (e.g., editing a scanned prescription or ID template), separate from the ATM/financial-fraud thread.

Finding 21, Five Most Recently Used Run Commands

Purpose: Recovers the most recently executed Run-box commands, which can reveal direct system/registry access or use of remote-access tools shortly before key events in the case.

Source 1: Autopsy

Registry path: `NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU`

Result: By MRUList order (most-recent first): regedt32, explorer, devmgmt.msc, calc, www.sourceforge.net.

un Programs 18 Results

Table Thumbnail Summary

Save Table as CSV

Source Name	S	C	O	Program Name	Path	Date/Time	Count	Comment
DEFRAG.EXE-738093E8.pf				DEFRAG.EXE	/WINDOWS/SYSTEM32	2007-09-27 17:09:36 PKT	35	Prefetch File
DFRGNTFS.EXE-4F838A89.pf				DFRGNTFS.EXE	/WINDOWS/SYSTEM32	2007-09-27 17:09:36 PKT	57	Prefetch File
DLLHOST.EXE-71214090.pf				DLLHOST.EXE	/WINDOWS/SYSTEM32	2007-09-27 18:09:17 PKT	238	Prefetch File
CONSENT.EXE-65F6206D.pf				CONSENT.EXE	/WINDOWS/SYSTEM32	2007-09-27 18:10:25 PKT	140	Prefetch File
DLLHOST.EXE-893DDF55.pf				DLLHOST.EXE	/WINDOWS/SYSTEM32	2007-09-27 18:10:27 PKT	257	Prefetch File
DLLHOST.EXE-CB3D53F2.pf				DLLHOST.EXE	/WINDOWS/SYSTEM32	2007-09-27 18:10:27 PKT	1	Prefetch File
EFSUI.EXE-DF03E0EF.pf				EFSUI.EXE	/WINDOWS/SYSTEM32	2007-09-27 18:10:27 PKT	68	Prefetch File

Figure 85. Prefetch/Run Programs listing referenced in Autopsy for this item.

Source 2: RegRipper (NTUSER.DAT)

Result: runmru plugin confirms MRUList = qponmlkjihgfedcba, LastWrite 2008-02-12 19:28:02Z; full history also includes c:\gdisk32.exe, mstsc, and two non-standard URLs (www.hellokitty.com, www.bigbadandugly.com).

```
runmru v.20201005
(NTUSER.DAT) Gets contents of user's RunMRU key
MITRE: T1204 (execution)

RunMru
Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
LastWrite Time 2008-02-12 19:28:02Z
MRUList = qponmlkjihgfedcba
a   cmd\1
b   mstsc\1
c   www.google.com\1
d   mspaint\1
e   msconfig\1
f   c:\gdisk32.exe\1
g   mmc\1
h   notepad\1
i   defrag\1
j   regedt32 12:23 /interactive\1
k   www.hellokitty.com\1
l   www.bigbadandugly.com\1
m   www.sourceforge.net\1
n   calc\1
o   devmgmt.msc\1
p   explorer\1
q   regedt32\1
----------------------------------------
1202844482|REG|||RunMRU: regedt32\1
----------------------------------------
```

Figure 86. runmru plugin output with the full Run-command history.

Source 3: Host Registry Comparison

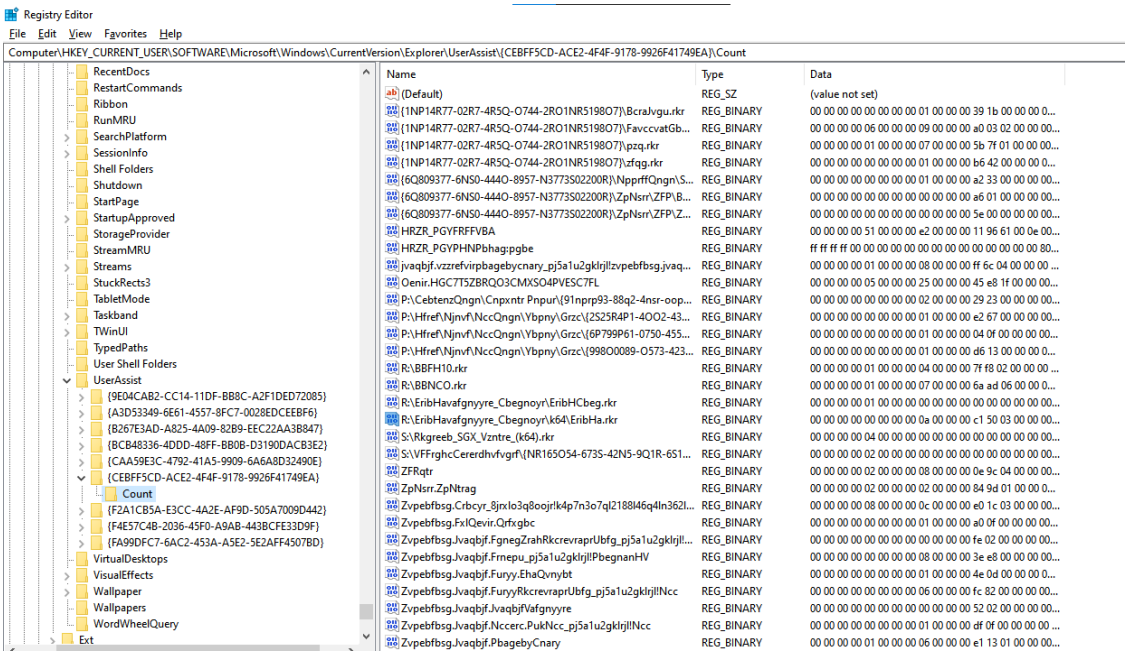


Figure 87. RunMRU key structure on the host comparison system.

> **EVIDENCE NOTE: FORENSIC SIGNIFICANCE**
>
> regedt32 and devmgmt.msc as the two most recent Run commands show the user directly accessing the Registry Editor and Device Manager shortly before the 2008-02-12 failed-login events in Finding 17–18, consistent with manual system/registry inspection during that session. mstsc (Remote Desktop Connection client) and gdisk32.exe (a disk-partitioning/wiping utility) are also worth flagging as anti-forensic-adjacent tool usage.

Finding 22, File Path for ATM_THEFTS1.ppt

Purpose: Resolves the exact file-system location(s) of a file named in a way that is directly relevant to the case narrative, to determine where it can be recovered from.

Source 1: Autopsy

Registry path: `NTUSER.DAT\Software\Microsoft\Office\PowerPoint\Recent File List`

Result: File1: E:\Business Idea\ATM_THEFTS1.ppt; File2: C:\Users\Wes Mantooth\Desktop\ATM_THEFTS1.ppt, the file exists in two locations: an external/removable E: drive and the user's own Desktop.

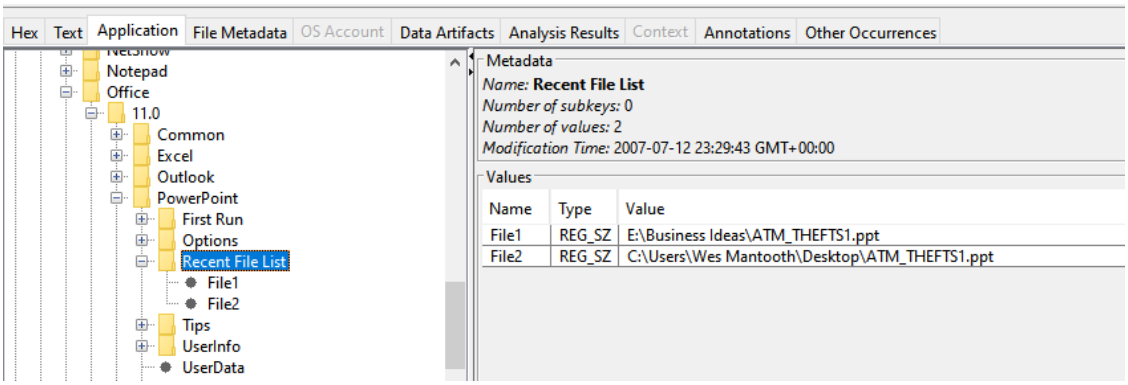


Figure 88. PowerPoint Recent File List entries resolving both paths for ATM_THEFTS1.ppt, in Autopsy.

Source 2: RegRipper (NTUSER.DAT)

Result: OpenSavePidlMRU\ppt independently confirms: My Computer\E:\Business Ideas\ATM_THEFTS1.ppt (LastWrite 2007-07-12 23:28:57Z).

```
OpenSavePidlMRU\ppt
LastWrite Time: Thu Jul 12 23:28:57 2007
Note: All value names are listed in MRUListEx order.

  My Computer\E:\Business Ideas\ATM_THEFTS1.ppt
```

Figure 89. OpenSavePidlMRU\ppt plugin output confirming the same file path.

EVIDENCE NOTE: FORENSIC SIGNIFICANCE

A file explicitly named ATM_THEFTS1.ppt is one of the most directly case-relevant artifacts recovered in this examination. Its presence in two locations (a removable E: drive and the Desktop) suggests the user copied it locally for editing or review. Presence in a Recent Files MRU list proves the file was opened by this user profile, it does not by itself prove authorship or intent, an important distinction to preserve in any report.

Next step: locate and export the file itself, hash it, examine its metadata (author, creation/modified times, embedded revision history), and correlate its timestamps against the account activity in Finding 18.

Finding 23, Recommended Investigator Response to Finding 22

Purpose: Defines the concrete next investigative steps required to turn the file path recovered in Finding 22 into usable evidence.

Recovery of the file path alone is not sufficient to draw conclusions. The recommended next steps are to: (1) locate and export the actual ATM_THEFTS1.ppt file from the image (both the E:\Business Idea and Desktop copies) and confirm whether it still exists or must be recovered from unallocated space; (2) compute and record its cryptographic hash for the evidence log; (3) review its content and any embedded author/editing metadata; and (4) build a timeline correlating the file's creation/access dates against the SAM login activity identified in Findings 17–18 to establish who was logged in when the file was created or last modified.

Finding 24, Internet Explorer Start Page

Purpose: Identifies the browser's configured start page, part of establishing the user's typical browsing configuration.

Source 1: Autopsy

Registry path: `NTUSER.DAT\Software\Microsoft\Internet Explorer\Main  (Start Page)`

Result: Captured view shows the Internet Explorer Main configuration branch; the explicit Start Page string was not clearly legible in this capture and should be re-verified directly against the Start Page value on re-examination.

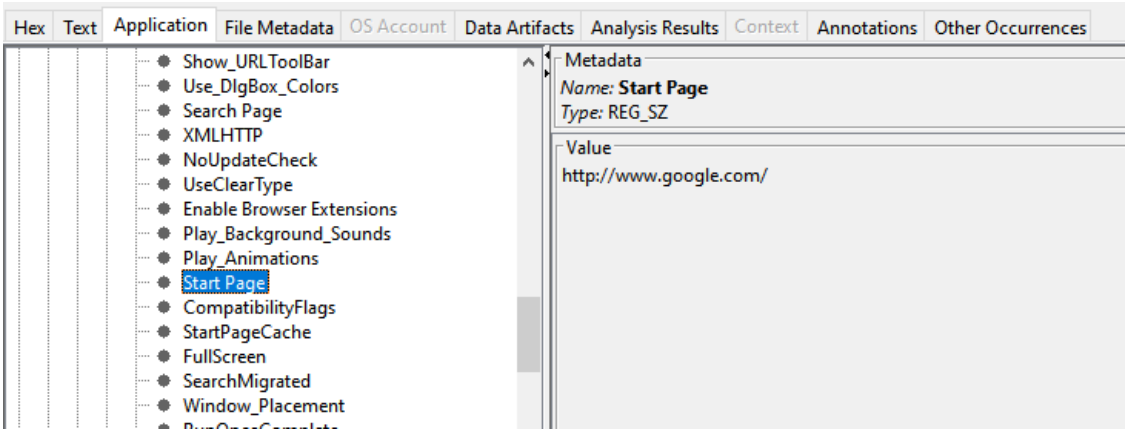


Figure 90. Internet Explorer Main key browsed in Autopsy.

Finding 25, Internet Explorer Default Download Directory

Purpose: Identifies where the browser was configured to save downloaded files, relevant to locating any downloaded evidence.

Source 1: Autopsy

Registry path: `NTUSER.DAT\Software\Microsoft\Internet Explorer\Main  (Download Directory)`

Result: Download Directory = C:\Users\Wes Mantooth\Desktop\... (a subfolder on the user's own Desktop, rather than the Windows default Downloads folder).

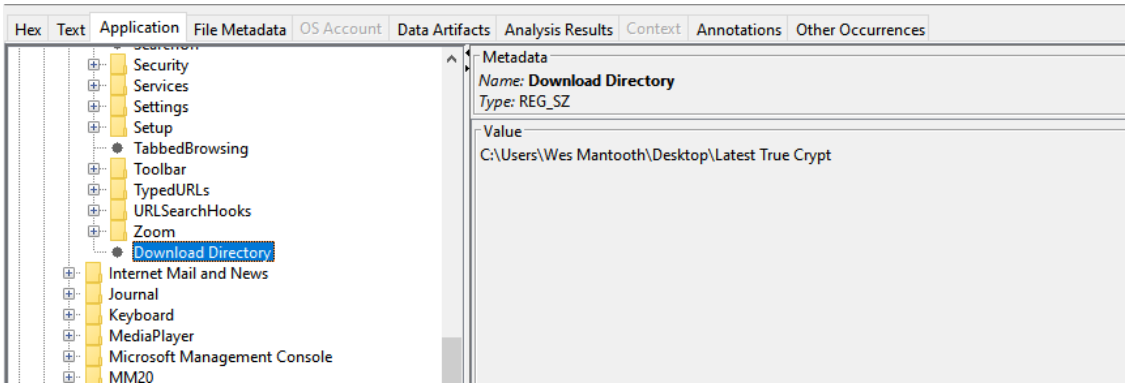


Figure 91. Download Directory value in Autopsy.

Finding 26, Internet Explorer Address-Bar / Favorites Activity

Purpose: Recovers the user's browser address-bar/favorites activity, to identify sites of investigative interest.

Examiner's note: the screenshot captured for this item shows the TypedURLs key (also used to answer Finding 32) rather than the IE Favorites list; no separate Favorites capture was available in the original worksheet.

Source 1: Autopsy

Registry path: `NTUSER.DAT\Software\Microsoft\Internet Explorer\TypedURLs`

Result: 25 TypedURLs entries recovered (see Finding 32 for the full breakdown); no dedicated Favorites subkey was captured separately.

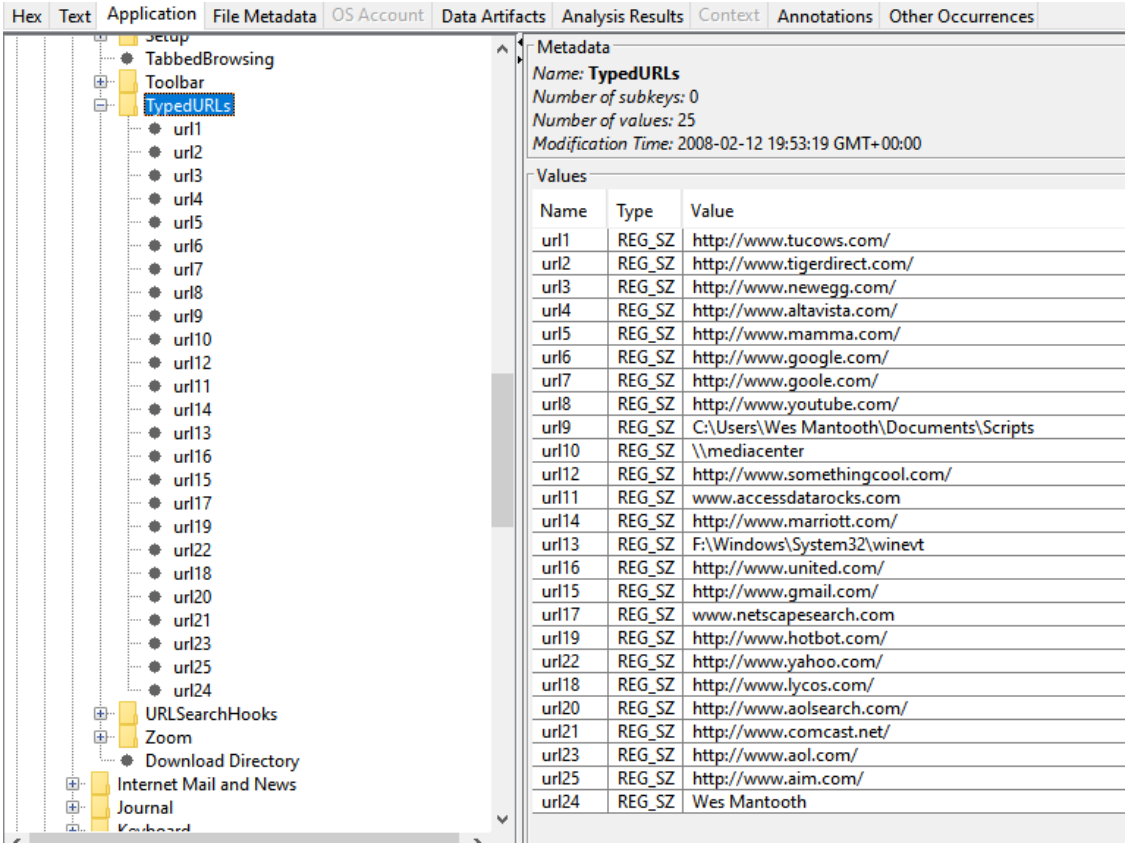


Figure 92. TypedURLs key entries in Autopsy, captured under this item.

Finding 27, Media Player Files Referenced from the F: Drive

Purpose: Identifies media files referenced from a removable drive letter, linking media-player activity back to the removable-device evidence identified earlier in this examination.

Source 1: Autopsy

Registry path: `NTUSER.DAT\Software\Microsoft\MediaPlayer\Player\RecentFileList`

Result: Two files on F:\, F:\Sounds and Video\wizoz18d.wav and F:\Sounds and Video\pf3.wav, alongside other RecentFileList entries on the E:\ (iPod_Control) and local C:\ drives.

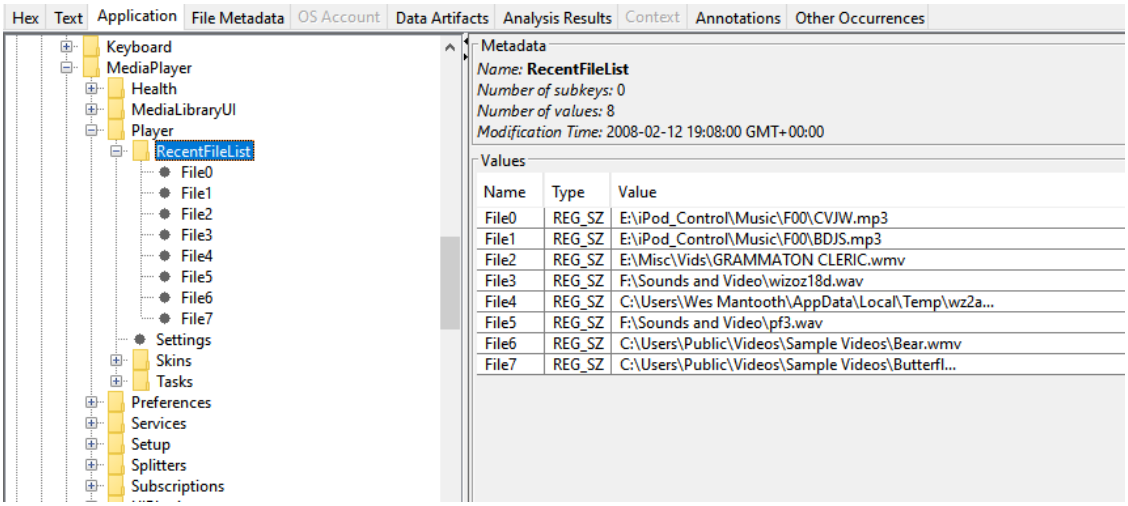


Figure 93. Windows Media Player RecentFileList entries in Autopsy, including the two F:\ .wav files.

EVIDENCE NOTE: FORENSIC SIGNIFICANCE

Media Player's RecentFileList records files by full path regardless of whether the referenced volume is still attached, which is why F:\, almost certainly a removable drive letter, appears here even though it is not the system volume. This directly links back to the removable-media activity identified in Finding 13.

Non-descriptive filenames (pf3.wav, wizoz18d.wav) on removable media are worth recovering and reviewing directly; steganographic or renamed-extension concealment is a common pattern worth ruling in or out.

Finding 28, Recommended Investigator Response to Finding 27

Purpose: Defines the concrete next investigative steps required to recover and verify the removable-media files referenced in Finding 27.

Because the F: drive is not part of the imaged system volume, the two referenced .wav files cannot be recovered from Mantooth.E01 directly. The recommended response is to: (1) identify which of the removable devices in Finding 13 was mapped to F: at the relevant time, using MountedDevices and drive-letter artifacts; (2) if that physical device is available as separate evidence, image and examine it directly; and (3) if not available, note the reference as an investigative lead rather than a confirmed artifact, since its content cannot be verified from this image alone.

Finding 29, Two Most Recent PowerPoint Files

Purpose: Confirms which presentation files were most recently accessed, cross-validating the file-path evidence recovered in Finding 22.

Source 1: Autopsy

Registry path: `NTUSER.DAT\Software\Microsoft\Office\PowerPoint\Recent File List`

Result: Both entries resolve to ATM_THEFTS1.ppt at its two locations: E:\Business Idea\ATM_THEFTS1.ppt and C:\Users\Wes Mantooth\Desktop\ATM_THEFTS1.ppt, no other .ppt files appear in the list.

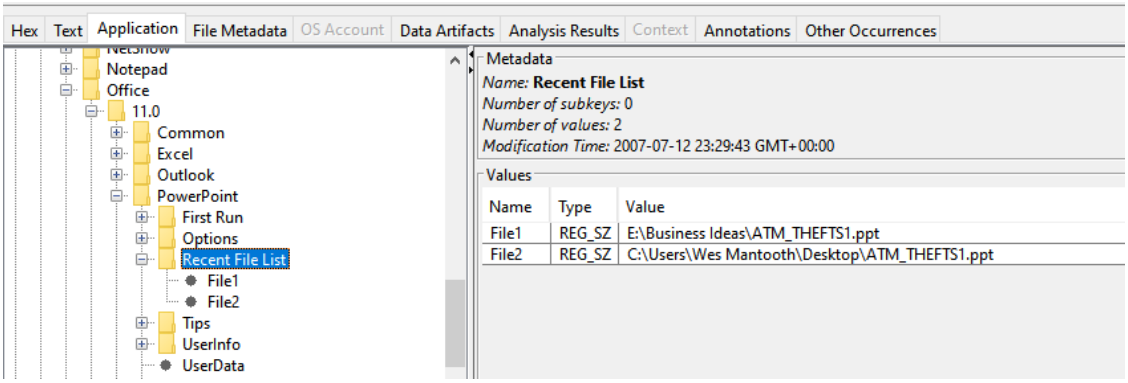


Figure 94. PowerPoint Recent File List in Autopsy, both entries are the two ATM_THEFTS1.ppt locations.

Finding 30, Five Items in the Recent Documents List and Their Investigative Value

Purpose: Reviews the user's complete Recent Documents history as a single body of evidence, to identify the full pattern of case-relevant files rather than just the one or two files already flagged individually.

The full RecentDocs MRU list for Wes Mantooth's profile (LastWrite 2008-02-12 21:38:57Z) was reviewed. Five items stand out as directly relevant to the case narrative:

1. Vista Mantooth Bitlocker Key 1.4.txt

Listed alongside a second, related entry “Wes Mantooth Image_Key Dustin.txt” and “Bitlocker Command.txt.txt”, locating encryption keys is a top priority during disk analysis. If encrypted volumes or BitLocker partitions are discovered elsewhere, a recovered plaintext key allows investigators to decrypt and analyze hidden evidence without brute-forcing it.

2. CC Nums.xls

A spreadsheet whose filename strongly implies a collection of credit card numbers. Analyzing this file helps establish motive related to identity theft or financial fraud; inspecting its metadata ($MACE timestamps, author fields) can also link the document to specific external sources or user actions.

3. ATM_THEFTS1.ppt

Covered in detail in Findings 22–23 and 29; its presence here confirms it as part of the same broad pattern of financially-themed documents.

4. BestCrypt Prefetch/Uninstall Evidence

BestCrypt 8.0 (Finding 14) is a commercial volume-encryption and data-wiping utility. Its presence, together with the TrueCrypt service entry in Finding 6, establishes a pattern of active use of more than one encryption tool, which is worth investigating for hidden or encrypted containers.

5. securityevt.evtx / testevt.evtx / Internet Explorer.evtx

Three separate exported/standalone Windows Event Log files appear in the Recent Documents list. Their presence suggests the user exported or copied log data for review, unusual end-user behavior that may indicate an attempt to review or tamper with audit evidence.

Broader review of the same MRU list also surfaced a cluster of filenames consistent with document forgery, “Prescription2.gif”, “doc-prescription.jpg”, “C money plates.doc”, and personal correspondence (“Dear Sweetie.doc”, “Dear Sweetie2.doc”). These fall outside the five items selected for priority review but are noted here as a lead for a fuller examination.

```
(NTUSER.DAT) Gets contents of user's RecentDocs key

RecentDocs
**All values printed in MRUList\MRUListEx order.
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
LastWrite Time: 2008-02-12 21:38:55Z
  100 = Tooth Docs
  101 = Wes.fang
  20 = WM.fang
  99 = WM.tooth
  81 = Vista Mantooth Bitlocker Key 1.4.txt
  71 = Wes Mantooth Image_Key_Dustin.txt
  75 = default
  74 = aim.ini
  98 = yahoo.ini
  4 = msn.ini
  55 = Secret Stuff
  15 = fun81.jpg
  32 = Funny Vids.zip
  97 = cathelmet.jpg
  96 = Jaws Cat.jpg
  54 = useles_cat.jpg
  10 = clean-dazed-kitty.jpg
  6 = My Internet Clearning Folder (\\mediacenter) (M:)
  95 = WASHER (F:)
  9 = New Text Document.txt
  31 = Misc Docs
  30 = You Got it!.txt
  94 = securityevt.evtx
  1 = testevt.evtx
  45 = Johns Stuff (\\TRAINING-KEN)
  93 = snaggle_kitty.jpg
  92 = key.bek
  91 = MANTOOTH (F:)
  90 = Enrollment approved for Web seminar Ken and Mitch's FTK 2 Test.htm
  82 = Logs
  19 = Internet Explorer.evtx
  88 = Juncion.exe
  89 = Junction v1_04.mht
  36 = How to create and manipulate NTFS junction points.mht
  14 = Family Pix
  23 = Dear ole Dad.jpg
  87 = Wes.jpg
  86 = Other Uncle Jon.jpg
  85 = Prefetch
```

Figure 95. Full RecentDocs MRUListEx enumeration in Autopsy, spanning the items discussed above.

```
84 = BESTCRYPT.EXE-7DE5BC83.pf
83 = Microsoft-Windows-ReadyBoost%4Operational.evtx
5 = Scripts
7 = nationaltall.bmp
16 = nationaltall.gif
25 = Prescription2.gif
27 = doc-prescription.jpg
26 = prescription.gif
80 = Bitlocker Command.txt.txt
79 = Mantooth Vista 1.4 Key.txt
78 = key.txt
77 = Removable Disk (E:)
76 = urls.txt.txt
73 = recbinDustin.ad1
72 = RECBIN Dustin.ad1
70 = recbin.ad1
12 = EFS DOCS
69 = John.doc
13 = Wes.doc
18 = CC Nums.xls
11 = C money plates.doc
68 = penguin_waiter_with_tray_sm_wht.gif
67 = Dear Sweetie2.doc
0 = Dear Sweetie.doc
66 = Ape_20shoot.gif
62 = Business Ideas
65 = ATM_THEFTS1.ppt
64 = Camera.bmp
63 = Guts.bmp
61 = untitled.bmp
59 = ~ar1730.xar
58 = Those who owes.xls
60 = Excel
57 = new
56 = edb00007.log
17 = Car Titles
3 = seanbefore
2 = Checks
53 = seanbefore.zip
33 = Local Disk (C:)
52 = mykey.txt
51 = Worker
50 = WorkerLog.txt
49 = Super Secret Stuff.zip
8 = Super Secret Stuff
48 = ar_test_نقيصة.doc
47 = russ_4_ящеркой.doc
46 = russ_2_Абажурный.doc
```

Figure 96. Full RecentDocs MRUListEx enumeration in Autopsy, spanning the items discussed above.

```
46 = russ_2_Абажурный.doc
44 = burgerkingandronald.gif
43 = 101MSDCF
39 = Pix
42 = Bill_Gates.gif
34 = Sounds and Video
28 = order851797-2007-04-12-13-17-02 (1).pdf
40 = funny.png
24 = Z169PCHK_e.gif
22 = C01VNCCHK_e.gif
21 = 91064B.gif
41 = order851797-2007-04-12-13-17-02.pdf
38 = Mr Smee
37 = 165183.html
35 = Removable Disk (F:)
29 = restoredsalty
```

Figure 97. Full RecentDocs MRUListEx enumeration in Autopsy, spanning the items discussed above.

EVIDENCE NOTE: CASE ASSESSMENT: FINDING 30

Taken together, these items form a coherent pattern: financial data (CC Nums.xls), a related fraud narrative document (ATM_THEFTS1.ppt), signs of anti-forensic behavior (a BitLocker key export, BestCrypt installation, and exported Security-log files), and a separate possible document-forgery thread (prescription-themed image files). This is the strongest single piece of evidence in the examination that the user was both handling sensitive financial data and taking active steps to protect or conceal it.

Recommended priority order for follow-up: (1) recover and hash CC Nums.xls and ATM_THEFTS1.ppt; (2) attempt to locate the BitLocker-protected volume and apply the recovered key; (3) search for BestCrypt/TrueCrypt container files; (4) review the exported .evtx files for signs of log tampering; (5) examine the prescription-themed image files as a possible secondary forgery lead.

Finding 31, Five Programs Listed in the Run/RunMRU Key

Purpose: Recovers a secondary view of recently executed Run-box commands, to corroborate Finding 21 with a fuller command history.

Source 1: Autopsy

Registry path: `NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU`

Result: Raw RunMRU values: a=cmd, b=mstsc, c=www.google.com, d=mspaint, e=msconfig (MRUList order q,p,o,n,m ranks regedt32, explorer, devmgmt.msc, calc, and sourceforge.net as most recent, see Finding 21).

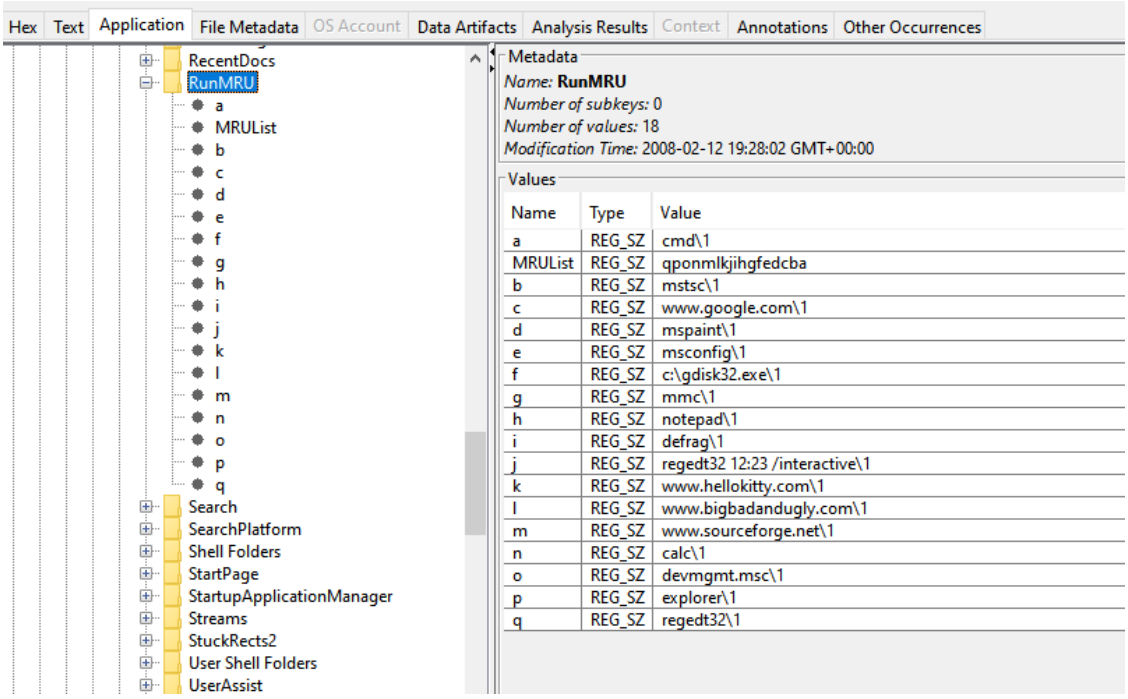


Figure 98. RunMRU raw values a–q in Autopsy.

Source 2: RegRipper (NTUSER.DAT)

Result: runmru plugin corroborates the identical 17-entry list and MRUList order.

```
runmru v.20201005
(NTUSER.DAT) Gets contents of user's RunMRU key
MITRE: T1204 (execution)

RunMru
Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
LastWrite Time 2008-02-12 19:28:02Z
MRUList = qponmlkjihgfedcba
a   cmd\1
b   mstsc\1
c   www.google.com\1
d   mspaint\1
e   msconfig\1
f   c:\gdisk32.exe\1
g   mmc\1
h   notepad\1
i   defrag\1
j   regedt32 12:23 /interactive\1
k   www.hellokitty.com\1
l   www.bigbadandugly.com\1
m   www.sourceforge.net\1
n   calc\1
o   devmgmt.msc\1
p   explorer\1
q   regedt32\1
```

Figure 99. runmru plugin output confirming the Run command history.

Finding 32, Five URLs Typed into Internet Explorer

Purpose: Recovers the addresses the user manually typed into the browser, which can reveal sites not present in normal browsing/favorites history.

Source 1: Autopsy

Registry path: `NTUSER.DAT\Software\Microsoft\Internet Explorer\TypedURLs`

Result: url1–url5: http://www.tucows.com/, http://www.tigerdirect.com/, http://www.newegg.com/, http://www.altavista.com/, http://www.mamma.com/ (25 entries total; later entries include a non-http path F:\Windows\System32\winevt, notable given the exported .evtx files in Finding 30).

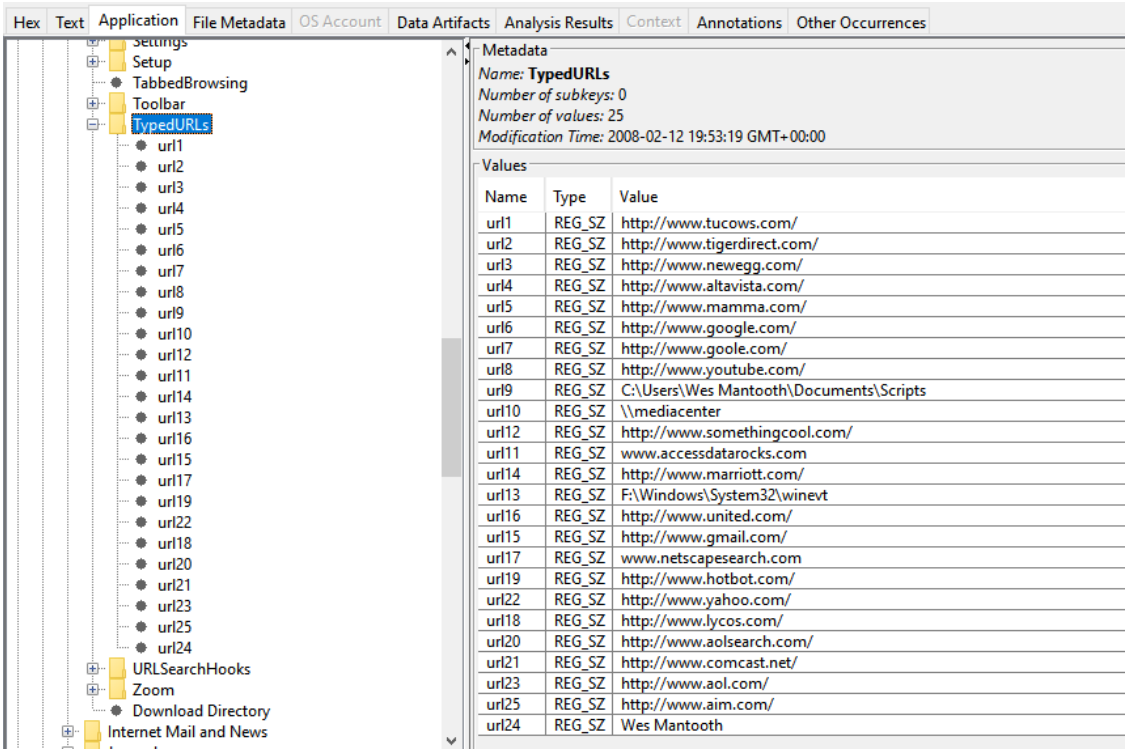


Figure 100. TypedURLs key entries in Autopsy.

Source 2: RegRipper (NTUSER.DAT)

Result: typedurls plugin confirms all 25 entries verbatim, LastWrite 2008-02-12 19:53:19Z, including url24 = “Wes Mantooth” (a non-URL entry, likely a mistyped search or name).

```
TypedURLs
Software\Microsoft\Internet Explorer\TypedURLs
LastWrite Time 2008-02-12 19:53:19Z
  url1 -> http://www.tucows.com/
  url2 -> http://www.tigerdirect.com/
  url3 -> http://www.newegg.com/
  url4 -> http://www.altavista.com/
  url5 -> http://www.mamma.com/
  url6 -> http://www.google.com/
  url7 -> http://www.goole.com/
  url8 -> http://www.youtube.com/
  url9 -> C:\Users\Wes Mantooth\Documents\Scripts
  url10 -> \\mediacenter
  url11 -> www.accessdatarocks.com
  url12 -> http://www.somethingcool.com/
  url13 -> F:\Windows\System32\winevt
  url14 -> http://www.marriott.com/
  url15 -> http://www.gmail.com/
  url16 -> http://www.united.com/
  url17 -> www.netscapesearch.com
  url18 -> http://www.lycos.com/
  url19 -> http://www.hotbot.com/
  url20 -> http://www.aolsearch.com/
  url21 -> http://www.comcast.net/
  url22 -> http://www.yahoo.com/
  url23 -> http://www.aol.com/
  url24 -> Wes Mantooth
  url25 -> http://www.aim.com/
```

Figure 101. typedurls plugin output listing all 25 recovered entries.

Finding 33, Email Addresses / Usernames Associated with Mantooth

Purpose: Identifies email addresses or messaging usernames associated with the primary user account, which is useful for correlating with other communications evidence.

Source 1: Autopsy

Registry path: `NTUSER.DAT\Software\Yahoo\Pager`

Result: Yahoo! Pager configuration resolves the account/username incisorman420, consistent with the Yahoo! Messenger username in Finding 35.

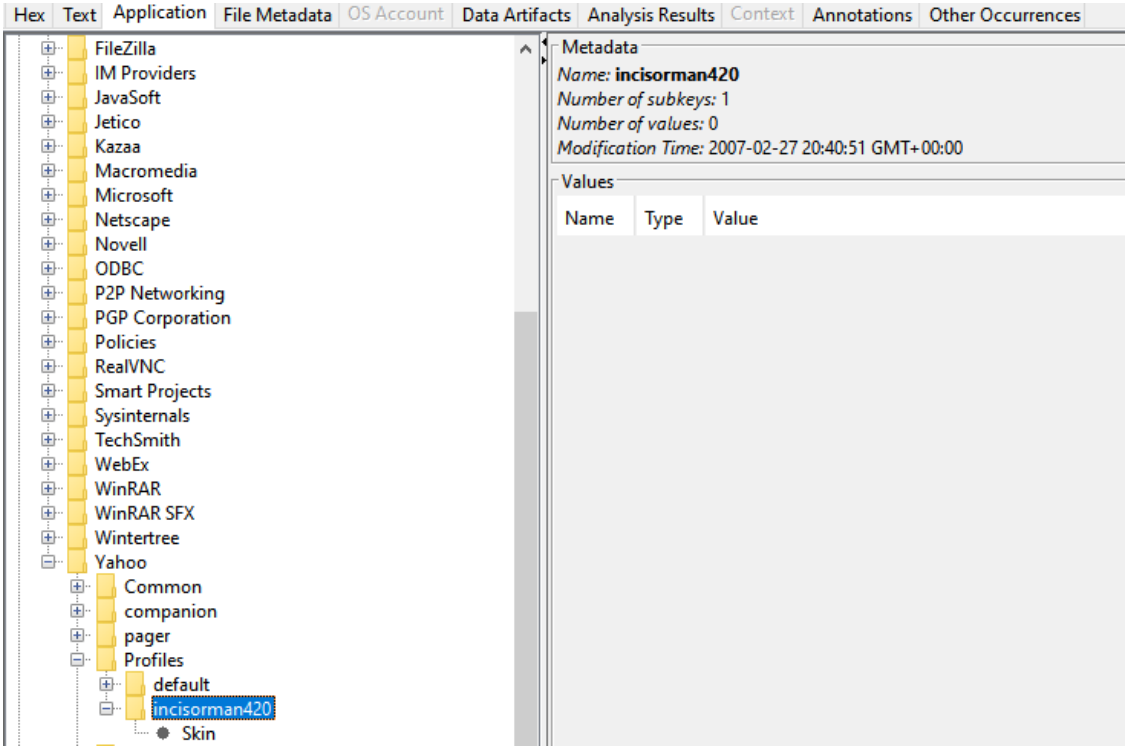


Figure 102. Yahoo account configuration keys in Autopsy resolving the username incisorman420.

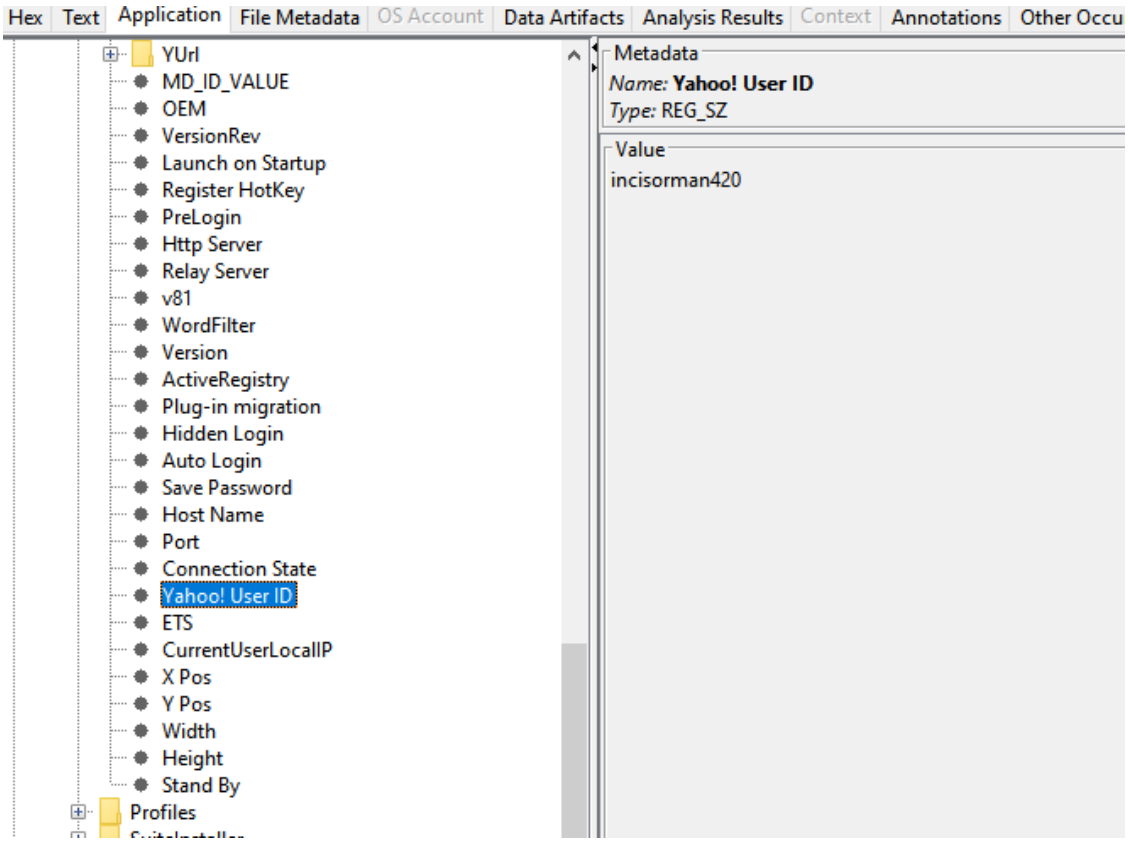


Figure 103. Yahoo account configuration keys in Autopsy resolving the username incisorman420.

Finding 34, WinVNC Remote Access Password

Purpose: Determines whether the system was configured for remote access via VNC, and whether the stored credential can be recovered, which is directly relevant to assessing whether the machine could have been accessed by a third party.

Source 1: Autopsy

Registry path: `SOFTWARE\RealVNC\WinVNC4`

Result: An 8-byte obfuscated Password value is present (Type: VncAuth); PortNumber 5900; Hosts filter restricts connections to +,192.168.1.103/255.255.255.255, i.e. only a single specific host is permitted to connect.

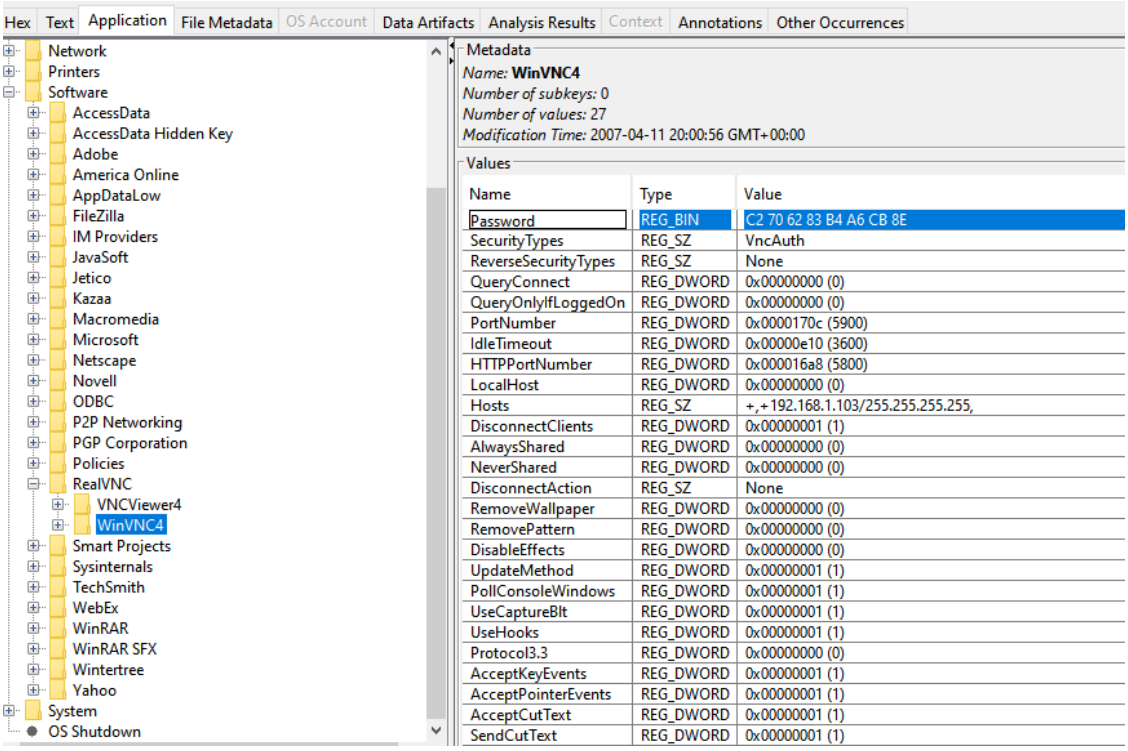


Figure 104. WinVNC4 configuration key in Autopsy, including the obfuscated Password value and Hosts filter.

EVIDENCE NOTE: FORENSIC SIGNIFICANCE

WinVNC (and its RealVNC successor) historically obfuscates its stored password using DES with a fixed, publicly documented key, meaning the stored value is reversible with widely available tools, not genuinely secure encryption. This examination confirmed the value is present and DES-obfuscated but did not conclusively recover a printable plaintext from the captured bytes; the raw 8-byte value should be re-extracted directly from the hive and decoded with the standard fixed VNC key on re-examination.

The presence of a configured VNC server, restricted to a single host IP, indicates this machine was set up to accept remote-desktop connections from one specific counterpart. Combined with the anti-forensic and financial-fraud indicators elsewhere in this examination, this is worth investigating as a possible remote-access arrangement between two parties.

Recommended step: decode the stored password using the known VNC DES key directly from the raw hive bytes and document the recovered credential in the evidence log; check for inbound connection logs or firewall rule changes coinciding with the service's configuration.

Finding 35, Yahoo Messenger Username

Purpose: Confirms the user's Yahoo Messenger identity, corroborating the account identification recovered in Finding 33.

Source 1: Autopsy

Registry path: `NTUSER.DAT\Software\Yahoo\Pager (Yahoo! User ID)`

Result: Yahoo! User ID = incisorman420.

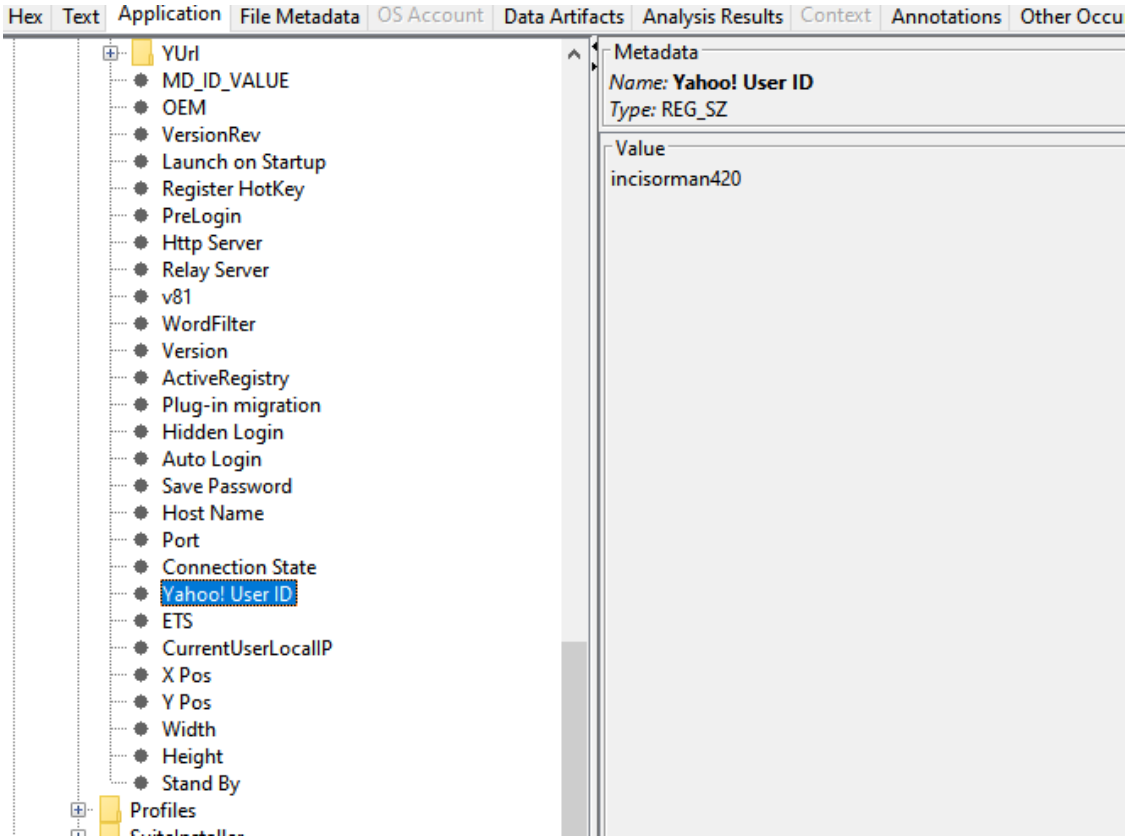


Figure 105. Yahoo! User ID value in Autopsy.

Finding 36, Default Printer Details

Purpose: Identifies the system's configured printer(s), completing the hardware/peripheral inventory of the machine.

Source 1: Autopsy

Registry path: `SOFTWARE\Microsoft\Windows NT\CurrentVersion\Devices`

Result: Installed printer devices include Microsoft XPS Document Writer and Microsoft Office Document Image Writer, alongside a physical Epson model; the explicit “default” flag was not clearly legible in this capture and should be re-verified against the Windows\Device value on re-examination.

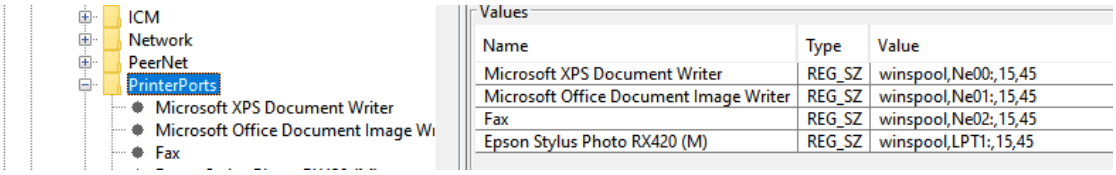


Figure 106. Devices key listing installed printers in Autopsy.

5. Case Assessment and Investigative Conclusions

The 36 registry findings, taken individually, establish routine system facts: hostname, time zone, installed hardware and software, network configuration, and user account structure. Their

investigative value emerges when read together against the account-activity and file-activity findings.

5.1 Account Activity

Wes Mantooth is confirmed as the primary account of interest (Finding 18), with an active, day-to-day usage pattern. The Dracula account's failed login within roughly one second of Wes Mantooth's own login event (Finding 17) is close enough in time to warrant a full logon-timeline reconstruction using the Security event log, rather than being dismissed as coincidence.

5.2 Financial-Crime Indicators

Three artifacts, considered together, form the strongest evidentiary thread in this examination: a spreadsheet named consistently with stored credit card numbers (CC Nums.xls), a presentation titled ATM_THEFTS1.ppt, and its resolved file path (Findings 22, 29–30). None of these prove wrongdoing on their own, a filename is not content, but they establish clear priorities for content recovery and review.

5.3 Anti-Forensic / Concealment Indicators

Multiple independent artifacts point toward active use of encryption and remote-access tools: a registered TrueCrypt service (Finding 6), Prefetch evidence of BestCrypt execution and a BitLocker recovery key export (Finding 30), and a configured WinVNC remote-access server with a recoverable password (Finding 34). A user handling sensitive financial filenames who is also actively encrypting data and exporting recovery keys is a pattern that, in a real investigation, would justify prioritizing full-disk unallocated-space carving and a dedicated search for encrypted container files.

5.4 Recommended Next Steps

- Recover, hash, and review the contents of CC Nums.xls and ATM_THEFTS1.ppt.
- Attempt to locate the BitLocker-protected volume referenced by the recovered recovery key.
- Search unallocated space and the file system for TrueCrypt/BestCrypt container files.
- Reconstruct a combined logon timeline for the Wes Mantooth and Dracula accounts using the Security event log.
- Decode and log the WinVNC password, and check for any inbound remote-access connection history.
- Treat the securityevt.evtx reference in Finding 30 as a possible log-tampering indicator and review the full Security log for gaps or clearing events.

5.5 Methodology Note

Every finding above was corroborated across at least two independent sources (Autopsy and RegRipper-parsed hive output), with a live host system used as a behavioral baseline wherever the artifact type allowed for it. No finding in this report relies on a single tool's interpretation alone.

Appendix A, Registry Hive and Key Reference

Base hive locations extracted from the Mantooth.E01 image for offline RegRipper analysis:

Hive	Source Path
`SAM`	...\Windows\System32\config\SAM
`SECURITY`	...\Windows\System32\config\SECURITY

SOFTWARE	...\Windows\System32\config\SOFTWARE
SYSTEM	...\Windows\System32\config\SYSTEM
NTUSER.DAT (Wes Mantooth)	...\Users\Wes Mantooth\NTUSER.DAT
NTUSER.DAT (Dracula)	...\Users\Dracula\NTUSER.DAT

Key registry paths referenced across findings:

Finding	Registry Path
1	SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName
2	SYSTEM\CurrentControlSet\Control\TimeZoneInformation
5	SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters
6	SYSTEM\CurrentControlSet\Services\TrueCrypt
7	SYSTEM\CurrentControlSet\Control\Windows (ShutdownTime)
8, 9, 13	SYSTEM\CurrentControlSet\Enum\USBSTOR
12	SOFTWARE\Microsoft\WZCSVC\Parameters\Interfaces\{GUID} (offset 0x47)
14, 15	SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall / CurrentVersion
16	SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList
17, 18	SAM\SAM\Domains\Account\Users
19, 20, 21, 29, 30	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs / ComDlg32
22, 23	NTUSER.DAT ...\RecentDocs (resolved MRU path)
24, 25	NTUSER.DAT\Software\Microsoft\Internet Explorer\Main
26	NTUSER.DAT\Software\Microsoft\Internet Explorer\Favorites
27, 28	NTUSER.DAT\Software\Microsoft\MediaPlayer\Player\RecentFileList
31	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run
32	NTUSER.DAT\Software\Microsoft\Internet Explorer\TypedURLs
34	SOFTWARE\RealVNC\WinVNC4 (Password)
35	NTUSER.DAT\Software\Yahoo\Pager
36	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Devices / Windows (Device)

Appendix B, Tools and Versions

Tool	Version / Notes
Autopsy	4.23.1, primary case platform for the Mantooth.E01 image
AccessData FTK Imager	Used to browse the image and export registry hives
RegRipper	3.0 (master branch), plugin-based offline hive parsing
Windows Registry Editor (regedit)	Native to host OS, used for live baseline comparison

Source worksheets: “Week 1, Windows Registry Practical” (question set) and “System Forensic” (worked answers and screenshots), both authored by the examiner as part of DFCS/CCFA coursework.