

New AUX assigned for the Analysis of two Desktop Computers

Review AUX Request in LIMA

Search Authority is Administrative

Images Received from ASAC [REDACTED]

Sent via Apricorn Drive

Images:

Z6E8KD3N.E01

JP1572JE36LSNK.E01

Working Copies Created

Working Copies Verified

Z6E8KD3N.E01

Image Verification Results:

Verification started: Mon Sep 16 14:03:21 2019

Verification finished: Mon Sep 16 14:44:51 2019

MD5 checksum: 629694386155e0f49e7a8c0da0da2840 : verified

SHA1 checksum: 3ac4c0fa2b1cb97020e22bc3966d4b3609c89d57 : verified

JP1572JE36LSNK.E01

Image Verification Results:

Verification started: Mon Sep 16 14:03:23 2019

Verification finished: Mon Sep 16 14:45:30 2019

MD5 checksum: 0dd9c2ad818c4a5a58bab2f78d57f2d7 : verified

SHA1 checksum: 0d78251b33302e327c56c1ef28e9ccc8f353bd46 : verified

Forensic Workstation X26958 utilized for forensic examination.

Forensic Software Utilized:

EnCase 8.10.00.209

FTK 7.1.0.290

AXIOM 3.7.0.16279

Images Added to EnCase

Verified in EnCase

Updated Time Zone Information (EST)

Search for Volume Shadow Copies

No Volume Shadows Found for either Device

Verified Volume Shadows in FTK

None Found

Process both Devices in EnCase

Recover Folders

Reconstruct folder structure of NTFS 3.0 files

File signature analysis

Protected file analysis

Thumbnail creation

Hash analysis

MD5

SHA1

Expand compound files

Find email

PST (Microsoft Outlook)

OST(Microsoft Outlook)

NSF (Lotus Notes)

DBX(Microsoft Outlook Express)

EDB(Microsoft Exchange)

AOL

MBOX

EMLX

Find Internet artifacts

Search unallocated space for Internet Artifacts (True)

Jeffrey Edward Epstein

Jeffery

Edward

Epstein
76318-054
Reyes
Index text and metadata
System Info Parser
User Activity
Operating System
Hardware
Software
Accounts/Users
Network
Shared/Mapped Devices
USB Devices
Network Shares
AutoRuns

PROCESSING COMPLETED SUCCESSFULLY

Images Processed in AXIOM

Z6E8KD3N.E01

AXIOM 3.7.0.16279 Copyright 2009-2020 Magnet Forensics® Inc.

Build 3.7.0.16279

Case Number: 2019-010614

Case Type: Other

Examiner: LITS [REDACTED] [REDACTED]

Case Information Generated At: Jan 08, 2020 08:23:28

Operating System: Microsoft Windows NT 10.0.17134.0

Runtime Version: 4.0.30319.42000

Settings:

Remove duplicates enabled: True

Acquire image segmentation enabled: False

Acquire image segmentation size: -1

Acquire image hashing enabled: True

Acquire image compression type: Fast

Acquire device cleanup enabled: True

Search Alerts entered: 6

Keywords entered: 6

Keyword regex count: 0

Dynamic app finder enabled: False

Picture and video categorization enabled: False

Files skipping by hash enabled: False

Case logo configured: True

Search archives: True

Search mobile backups: True
Max nested container depth: 5
Output Folder: F:\2019-010614\AXIOM Second Request\Z6E8KD3N\

Z6E8KD3N.E01 - Partition 1 (Microsoft NTFS, 461.1 GB)

Evidence number: Z6E8KD3N

Searches selected:

- pagefile.sys
- swapfile.sys
- \$MFT
- \$LogFile
- hiberfil.sys
- Volume Shadow Copies
- Unallocated Clusters
- File Slack Space
- All Files and Folder
- Uninitialized File Area

Z6E8KD3N.E01 - Unpartitioned Space

Evidence number: Z6E8KD3N

Searches selected:

- Unpartitioned Space

Search items selected:

- Platform: Computer
- \$LogFile Analysis
- 360 Safe Browser
- Adium
- Adobe Flash Cookies / Local Shared Objects
- AIM
- AmCache
- Android Backups
- Application Install States
- Ares
- Audio
- AutoRun Items
- Bebo
- Bing Toolbar
- Bitcoin
- BitLocker Recovery Key
- Calc
- Calendar Events (ics)
- Carbonite
- Carved Archives (content not searched)

Carved Audio
Chatroulette
Chatstep
Chrome
Cortana
CSV Documents
Dropbox
DS_Store
Edge/Internet Explorer
EGG Archives
EML(X) Files
Emule
Encrypted Files
Encryption / Anti-forensics Tools
Excel
Facebook
File System Information
Firefox
Flickr
Gigatribe v2 and v3
Gmail
GMX Webmail
Google Analytics
Google Docs
Google Drive
Google Maps
Google Talk
Google Toolbar
Google WebP Images
Google+
Hangul Word Processor
Hotmail Webmail
Hushmail
iChat
ICQ
IME Suggestions
iMessage
Impress
Instagram
Installed Programs
iOS Backups
IP Addresses - Audio/Video Calls
ISO Files
Jump Lists

KakaoTalk
Keyword Searches
Known DLLs
Limerunner
Limewire / Frostwire
LINE
LinkedIn
LNK Files
Luckywire
Lync / Office Communicator
Mail.ru
Mailinator
Malware/Phishing URLs
MBOX E-mails
mIRC
Most Recently Used
MSN Plus!
MUICache
MySpace
Network Interfaces
Network Profiles
Network Share Information
Network Usage
Notification Center
Omegle
OneDrive
ooVoo
Opera
Operating System Information
Outlook
Outlook Web App
Outlook Webmail
Paltalk
PDF
Photoshop Files
Pictures
Pidgin
Pornography URLs
Potential Browser Activity (Incl. Private/ Incognito URLs)
PowerPoint
Prefetch Files
QQ
QuickBooks Files
RealPlayer

Rebuild Webpages
Recycle Bin
Remote Desktop Protocol
RTF Documents
Safari
Scheduled Tasks
Second Life
Services
Shareaza
SharePoint
Shellbags
Shim Cache
Sina Weibo
Skype
SRUM
Startup Items
Text Documents
Timezone Information
TorChat
Torrents
Trillian
Twitter
USB Devices
Usenet Binary Files
User Accounts
UserAssist
Viber
Videos
Virtual Machines
VK
VLC Media Player
Web Video Fragments
WebKit
WeChat
WhatsApp
Windows Event Logs
Windows Live Messenger / MSN Messenger®
Windows Logon Banner
Windows Mail
Windows Timeline
Word
WordPerfect Files
World of Warcraft
Writer

Xbox Internet Explorer History
Yahoo! Messenger
Yahoo! Webmail
Your Phone
Zoom

Summary:

Start Time: Jan 08, 2020 08:23:28
End Time: Jan 09, 2020 02:20:08
Search Duration: 17:56:30
Indexing Duration: 00:01:06
Search Outcome: Success

Final results of search:

\$LogFile Analysis: 15793 items
AmCache Device Containers: 34 items
AmCache Driver Binaries: 262 items
AmCache Driver Packages: 14 items
AmCache File Entries: 662 items
AmCache Pnp Devices: 97 items
AmCache Program Entries: 150 items
AmCache Shortcuts: 719 items
Audio: 2240 items
AutoRun Items: 851 items
Carved Archives (content not searched): 9451 items
Carved Audio: 3080 items
Carved Video: 1285 items
Chrome Autofill: 28 items
Chrome Autofill Profiles: 1 items
Chrome Cache Records: 25506 items
Chrome Cookies: 848 items
Chrome Current Session: 10 items
Chrome Current Tabs: 5 items
Chrome FavIcons: 53 items
Chrome Keyword Search Terms: 1 items
Chrome Last Session: 9 items
Chrome Last Tabs: 3 items
Chrome Logins: 7 items
Chrome Top Sites: 2 items
Chrome Web History: 5 items
Chrome Web Visits: 11 items
Classifieds URLs: 103868 items
Cloud Services URLs: 71 items
CSV Documents: 12 items

Dating Sites URLs: 56 items
Edge/Internet Explorer 10-11 Content: 3163978 items
Edge/Internet Explorer 10-11 Cookies: 74039 items
Edge/Internet Explorer 10-11 Daily/Weekly History: 184489 items
Edge/Internet Explorer 10-11 Dependency Entries: 3884 items
Edge/Internet Explorer 10-11 Downloads: 43 items
Edge/Internet Explorer 10-11 Main History: 382359 items
Email Attachments: 10 items
EML(X) Files: 549 items
eMule GUIDs: 1 items
Encrypted Files: 172 items
Encryption / Anti-forensics Tools: 3 items
Excel Documents: 155 items
Facebook Chat: 209 items
Facebook Pages: 11 items
Facebook Status Updates/Wall Posts/Comments: 6 items
Facebook URLs: 4670 items
File Associations: 2191 items
File System Information: 1 items
Firefox Add-ons: 5 items
Firefox Bookmarks: 100 items
Firefox Cache Records: 19953 items
Firefox Cookies: 2554 items
Firefox FavIcons: 45 items
Firefox FormHistory: 10 items
Firefox Input History: 2 items
Firefox SessionStore Artifacts: 891 items
Firefox Web History: 1242 items
Firefox Web Visits: 1455 items
Flash Cookies: 5622 items
Google Analytics First Visit Cookies: 4942 items
Google Analytics First Visit Cookies Carved: 13075 items
Google Analytics Referral Cookies: 4669 items
Google Analytics Referral Cookies Carved: 11477 items
Google Analytics Session Cookies: 2719 items
Google Analytics Session Cookies Carved: 7193 items
Google Analytics URLs: 1955 items
Google Analytics URLs Carved: 404 items
Google Drive: 1 items
Google Maps: 903 items
Google Maps Queries: 301 items
Google Maps Tiles: 5131 items
Google Searches: 30921 items
Google WebP Images: 64 items

Hangul Word Processor: 2 items
Human Trafficking Site URLs: 7 items
Identifiers: 3848 items
IE InPrivate/Recovery URLs: 19981 items
Installed Microsoft Programs: 300 items
Installed Programs: 220 items
Internet Explorer Cache Records: 309421 items
Internet Explorer Cookie Records: 867 items
Internet Explorer Cookies: 256351 items
Internet Explorer Daily History: 595 items
Internet Explorer Favorites: 4336 items
Internet Explorer Leak Records: 343 items
Internet Explorer Main History: 1299 items
Internet Explorer Private Records: 19623 items
Internet Explorer Redirect Records: 25976 items
Internet Explorer Typed URLs: 1895 items
Internet Explorer Weekly History: 123 items
Jump Lists: 12004 items
Keyword Searches: 69 items
Known DLLs: 56 items
LNK Files: 31311 items
Locally Accessed Files and Folders: 61125 items
Malware/Phishing URLs: 33 items
MRU Folder Access: 315 items
MRU Opened/Saved Files: 1624 items
MRU Recent Files & Folders: 7459 items
MRU Run Commands: 3 items
MUICache: 23173 items
Network Interfaces (Registry): 2 items
Network Profiles: 2 items
Network Share Information: 730 items
Operating System Information: 2 items
Parsed Search Queries: 24131 items
Passwords and Tokens: 7 items
PDF Documents: 1280 items
Photoshop Files: 76 items
Pictures: 953022 items
Potential Browser Activity: 57165 items
Potential Facebook Pictures: 3923 items
PowerPoint Documents: 47 items
Prefetch Files - Windows XP/Vista/7: 179 items
QuickBooks Files: 115 items
Rebuilt Webpages: 45227 items
Remote Desktop Protocol: 66 items

RTF Documents: 1175 items
Safari History: 4 items
Shellbags: 10648 items
Shim Cache: 7 items
Shipping Site URLs: 2794 items
Social Media URLs: 6561 items
Startup Items: 263 items
System Services: 880 items
Tax Site URLs: 1060 items
Text Documents: 109494 items
Timezone Information: 1 items
Torrent URLs: 77 items
USB Devices: 126 items
User Accounts: 258 items
UserAssist: 9678 items
Videos: 5194 items
VLC Recently Played Files: 118 items
Web Chat URLs: 1 items
Web Video Fragments: 282 items
WebKit Browser Web History (Carved): 631 items
Windows Event Logs: 343316 items
Windows Logon Banner: 1 items
Word Documents: 1813 items
WordPerfect Files: 71 items
Yahoo! Non-Encrypted Chat: 938 items

JP1572JE36LSNK.E01

AXIOM 3.7.0.16279 Copyright 2009-2020 Magnet Forensics® Inc.

Build 3.7.0.16279

Case Number: 2019-010614

Case Type: Other

Examiner: LITS [REDACTED] [REDACTED]

Case Information Generated At: Jan 09, 2020 07:07:34

Operating System: Microsoft Windows NT 10.0.17134.0

Runtime Version: 4.0.30319.42000

Settings:

Remove duplicates enabled: True

Acquire image segmentation enabled: False

Acquire image segmentation size: -1

Acquire image hashing enabled: True

Acquire image compression type: Fast

Acquire device cleanup enabled: True

Search Alerts entered: 6

Keywords entered: 6
Keyword regex count: 0
Dynamic app finder enabled: False
Picture and video categorization enabled: False
Files skipping by hash enabled: False
Case logo configured: True
Search archives: True
Search mobile backups: True
Max nested container depth: 5
Output Folder: F:\2019-010614\AXIOM Second Request\JP1572JE36LSNK\

JP1572JE36LSNK.E01 - Partition 1 (EXT-family, 156.85 MB)

Evidence number: JP1572JE36LSNK

Searches selected:

- Unallocated Clusters
- All Files and Folder

JP1572JE36LSNK.E01 - Partition 2 (Microsoft NTFS, 95 MB) System Reserved

Evidence number: JP1572JE36LSNK

Searches selected:

- pagefile.sys
- swapfile.sys
- \$MFT
- \$LogFile
- hiberfil.sys
- Volume Shadow Copies
- Unallocated Clusters
- File Slack Space
- All Files and Folder
- Uninitialized File Area

JP1572JE36LSNK.E01 - Partition 3 (Microsoft NTFS, 465.51 GB)

Evidence number: JP1572JE36LSNK

Searches selected:

- pagefile.sys
- swapfile.sys
- \$MFT
- \$LogFile
- hiberfil.sys
- Volume Shadow Copies
- Unallocated Clusters
- File Slack Space
- All Files and Folder
- Uninitialized File Area

JP1572JE36LSNK.E01 - Unpartitioned Space

Evidence number: JP1572JE36LSNK

Searches selected:

Unpartitioned Space

Search items selected:

Platform: Computer

\$LogFile Analysis

360 Safe Browser

Adium

Adobe Flash Cookies / Local Shared Objects

AIM

AmCache

Android Backups

Application Install States

Ares

Audio

AutoRun Items

Bebo

Bing Toolbar

Bitcoin

BitLocker Recovery Key

Calc

Calendar Events (ics)

Carbonite

Carved Archives (content not searched)

Carved Audio

Chatroulette

Chatstep

Chrome

Cortana

CSV Documents

Dropbox

DS_Store

Edge/Internet Explorer

EKG Archives

EML(X) Files

Emule

Encrypted Files

Encryption / Anti-forensics Tools

Excel

Facebook

File System Information

Firefox
Flickr
Gigatribe v2 and v3
Gmail
GMX Webmail
Google Analytics
Google Docs
Google Drive
Google Maps
Google Talk
Google Toolbar
Google WebP Images
Google+
Hangul Word Processor
Hotmail Webmail
Hushmail
iChat
ICQ
IME Suggestions
iMessage
Impress
Instagram
Installed Programs
iOS Backups
IP Addresses - Audio/Video Calls
ISO Files
Jump Lists
KakaoTalk
Keyword Searches
Known DLLs
Limerunner
Limewire / Frostwire
LINE
LinkedIn
LNK Files
Luckywire
Lync / Office Communicator
Mail.ru
Mailinator
Malware/Phishing URLs
MBOX E-mails
mIRC
Most Recently Used
MSN Plus!

MUICache
MySpace
Network Interfaces
Network Profiles
Network Share Information
Network Usage
Notification Center
Omegle
OneDrive
ooVoo
Opera
Operating System Information
Outlook
Outlook Web App
Outlook Webmail
Paltalk
PDF
Photoshop Files
Pictures
Pidgin
Pornography URLs
Potential Browser Activity (Incl. Private/ Incognito URLs)
PowerPoint
Prefetch Files
QQ
QuickBooks Files
RealPlayer
Rebuild Webpages
Recycle Bin
Remote Desktop Protocol
RTF Documents
Safari
Scheduled Tasks
Second Life
Services
Shareaza
SharePoint
Shellbags
Shim Cache
Sina Weibo
Skype
SRUM
Startup Items
Text Documents

Timezone Information
TorChat
Torrents
Trillian
Twitter
USB Devices
Usenet Binary Files
User Accounts
UserAssist
Viber
Videos
Virtual Machines
VK
VLC Media Player
Web Video Fragments
WebKit
WeChat
WhatsApp
Windows Event Logs
Windows Live Messenger / MSN Messenger®
Windows Logon Banner
Windows Mail
Windows Timeline
Word
WordPerfect Files
World of Warcraft
Writer
Xbox Internet Explorer History
Yahoo! Messenger
Yahoo! Webmail
Your Phone
Zoom

Summary:

Start Time: Jan 09, 2020 07:07:34
End Time: Jan 09, 2020 23:01:40
Search Duration: 15:53:56
Indexing Duration: 00:01:03
Search Outcome: Success

Final results of search:

\$LogFile Analysis: 21601 items
AmCache Device Containers: 29 items
AmCache Driver Binaries: 267 items

AmCache Driver Packages: 19 items
AmCache File Entries: 820 items
AmCache Pnp Devices: 94 items
AmCache Program Entries: 157 items
AmCache Shortcuts: 585 items
Audio: 2995 items
AutoRun Items: 918 items
Carved Archives (content not searched): 9683 items
Carved Audio: 4655 items
Carved Video: 1376 items
Classifieds URLs: 84789 items
Cloud Services URLs: 57 items
CSV Documents: 18 items
Dating Sites URLs: 412 items
Edge/Internet Explorer 10-11 Content: 3274517 items
Edge/Internet Explorer 10-11 Cookies: 66140 items
Edge/Internet Explorer 10-11 Daily/Weekly History: 182627 items
Edge/Internet Explorer 10-11 Dependency Entries: 4610 items
Edge/Internet Explorer 10-11 Downloads: 69 items
Edge/Internet Explorer 10-11 Main History: 376240 items
Email Attachments: 11 items
EML(X) Files: 214 items
Encrypted Files: 128 items
Encryption / Anti-forensics Tools: 3 items
Excel Documents: 198 items
Facebook Chat: 374 items
Facebook Pages: 14 items
Facebook URLs: 3085 items
File Associations: 2172 items
File System Information: 3 items
Firefox Add-ons: 8 items
Firefox Bookmarks: 66 items
Firefox Cache Records: 9410 items
Firefox Cookies: 1479 items
Firefox Downloads: 71 items
Firefox FavIcons: 90 items
Firefox FormHistory: 5 items
Firefox Input History: 3 items
Firefox SessionStore Artifacts: 886 items
Firefox Web History: 1062 items
Firefox Web Visits: 1150 items
Flash Cookies: 4790 items
Gmail Fragments: 13 items
Gmail Webmail: 225 items

Google Analytics First Visit Cookies: 3370 items
Google Analytics First Visit Cookies Carved: 8883 items
Google Analytics Referral Cookies: 3181 items
Google Analytics Referral Cookies Carved: 7674 items
Google Analytics Session Cookies: 1807 items
Google Analytics Session Cookies Carved: 4483 items
Google Analytics URLs: 2240 items
Google Analytics URLs Carved: 657 items
Google Maps: 727 items
Google Maps Queries: 177 items
Google Maps Tiles: 2435 items
Google Searches: 20802 items
Google WebP Images: 35 items
Hangul Word Processor: 2 items
Human Trafficking Site URLs: 1 items
Identifiers: 3088 items
IE InPrivate/Recovery URLs: 152 items
Installed Microsoft Programs: 306 items
Installed Programs: 233 items
Internet Explorer Cache Records: 2 items
Internet Explorer Cookies: 220671 items
Internet Explorer Daily History: 2 items
Internet Explorer Favorites: 4507 items
Internet Explorer Main History: 7 items
Internet Explorer Typed URLs: 1682 items
Jump Lists: 12877 items
Keyword Searches: 121 items
Known DLLs: 56 items
LNK Files: 33257 items
Locally Accessed Files and Folders: 72708 items
Malware/Phishing URLs: 112 items
MRU Folder Access: 329 items
MRU Opened/Saved Files: 1740 items
MRU Recent Files & Folders: 7802 items
MRU Run Commands: 1 items
MUICache: 25441 items
Network Interfaces (Registry): 2 items
Network Profiles: 3 items
Network Share Information: 775 items
Operating System Information: 1 items
Parsed Search Queries: 21943 items
PDF Documents: 1613 items
Photoshop Files: 102 items
Pictures: 903684 items

Pornography URLs: 3 items
Potential Browser Activity: 45589 items
Potential Facebook Pictures: 3654 items
PowerPoint Documents: 31 items
Prefetch Files - Windows XP/Vista/7: 248 items
QuickBooks Files: 109 items
Rebuilt Webpages: 43866 items
Remote Desktop Protocol: 61 items
RTF Documents: 801 items
Safari History: 4 items
Shellbags: 19087 items
Shipping Site URLs: 1626 items
Social Media URLs: 5160 items
Startup Items: 285 items
System Services: 902 items
Tax Site URLs: 572 items
Text Documents: 91547 items
Timezone Information: 1 items
Torrent URLs: 23 items
Trillian: 6 items
USB Devices: 164 items
User Accounts: 271 items
UserAssist: 10360 items
Videos: 6061 items
VLC Recently Played Files: 45 items
Web Chat URLs: 5 items
Web Video Fragments: 15 items
WebKit Browser Web History (Carved): 251 items
Windows Event Logs: 345190 items
Windows Logon Banner: 1 items
Word Documents: 2066 items
WordPerfect Files: 24 items
Yahoo! Non-Encrypted Chat: 9 items

Build Timeline in AXIOM for both images

Z6E8KD3N.E01 Completed Successfully

JP1572JE36LSNK.E01 Completed Successfully

Perform Timeline Analysis for User Activity on the System for Z6E8KD3N.E01

Identified user for 08/09/2019 to 08/10/2019

User: [REDACTED]

Username: BOP18923

SID: S-1-5-21-1079978788-711783815-1788341251-1015

08/09/2019	16:05:07	User BOP18923 Successfully Logged onto the System
08/09/2019	16:07:47	User BOP18923 Successfully Reset their Password
08/09/2019	16:10:58	GroupWise (grpwise.exe) is launched.
08/09/2019	16:17:54	Internet Explorer (iexplorer.exe) is launched.
08/09/2019	16:17:59	Internet Activity Recorded
08/09/2019	16:18:00	Internet Activity Recorded
08/09/2019	16:18:42	Internet Activity Recorded
08/09/2019	16:29:54	Internet Explorer (iexplorer.exe) is launched.
08/09/2019	16:29:57	Internet Activity: "https://10.33.56.106/TRUACCESS"
08/09/2019	16:53:50	Screen Pass is Executed by System/User - Computer System is Locked
08/09/2019	17:11:40	User BOP18923 Successfully Unlocked the System
08/09/2019	17:25:53	Screen Pass is Executed by System/User - Computer System is Locked
08/09/2019	17:27:33	User BOP18923 Successfully Unlocked the System
08/09/2019	17:28:17	User launches GroupWise (grpwise.exe)
08/09/2019	17:32:58	Microsoft Access (MSACCESS.exe) is launched.
08/09/2019	17:54:24	Internet Activity Recorded
08/09/2019	17:54:44	Internet Activity Recorded
08/09/2019	17:54:46	Internet Activity Recorded
08/09/2019	17:57:58	Internet Activity Recorded
08/09/2019	17:58:42	Internet Activity Recorded
08/09/2019	18:00:57	Internet Activity Recorded
08/09/2019	18:02:38	Internet Activity Recorded
08/09/2019	18:02:47	Internet Activity Recorded
08/09/2019	18:09:34	Internet Explorer (iexplorer.exe) is launched.
08/09/2019	18:09:50	Internet Activity Recorded
08/09/2019	18:11:16	Internet Activity Recorded

08/09/2019	18:46:46	Screen Pass is Executed by System/User - Computer System is Locked
08/09/2019	18:47:52	User BOP18923 Successfully Unlocked the System
08/09/2019	18:59:38	Screen Pass is Executed by System/User - Computer System is Locked
08/09/2019	19:03:19	User BOP18923 Successfully Unlocked the System
08/09/2019	19:21:44	Screen Pass is Executed by System/User - Computer System is Locked
08/09/2019	19:38:44	User BOP18923 Successfully Unlocked the System
08/09/2019	19:57:45	Screen Pass is Executed by System/User - Computer System is Locked
08/09/2019	19:59:56	User BOP18923 Successfully Unlocked the System
08/09/2019	20:26:35	Screen Pass is Executed by System/User - Computer System is Locked
08/09/2019	20:42:12	User BOP18923 Successfully Unlocked the System
08/09/2019	20:52:37	Screen Pass is Executed by System/User - Computer System is Locked
08/09/2019	21:12:17	User BOP18923 Successfully Unlocked the System
08/09/2019	21:22:41	Screen Pass is Executed by System/User - Computer System is Locked
08/09/2019	21:30:34	User BOP18923 Successfully Unlocked the System
08/09/2019	21:39:49	GroupWise (grpwise.exe) is launched.
08/09/2019	21:56:40	Screen Pass is Executed by System/User - Computer System is Locked
08/09/2019	22:14:35	User BOP18923 Successfully Unlocked the System
08/09/2019	22:25:37	Screen Pass is Executed by System/User - Computer System is Locked
08/09/2019	22:27:46	User BOP18923 Successfully Unlocked the System
08/09/2019	22:30:58	GroupWise (grpwise.exe) is launched.
08/09/2019	22:31:24	Internet Explorer (iexplorer.exe) is launched.
08/09/2019	22:34:37	Internet Activity Recorded
08/09/2019	22:34:39	Internet Activity Recorded
08/09/2019	22:42:36	Internet Activity Recorded
08/09/2019	22:42:47	Internet Activity Recorded
08/09/2019	22:51:04	Internet Activity Recorded
08/09/2019	22:51:33	Internet Activity Recorded
08/09/2019	22:51:46	Internet Activity Recorded
08/09/2019	23:02:39	Internet Activity Recorded

08/09/2019	23:09:11	Internet Activity Recorded
08/09/2019	23:25:22	Internet Activity Recorded
08/09/2019	23:26:05	Internet Activity Recorded
08/09/2019	23:26:33	Internet Activity Recorded
08/09/2019	23:31:57	Internet Activity Recorded
08/09/2019	23:32:00	Internet Activity Recorded
08/09/2019	23:32:55	Internet Activity Recorded
08/09/2019	23:35:14	Internet Activity Recorded
08/09/2019	23:38:59	Internet Activity Recorded
08/09/2019	23:39:01	Internet Activity Recorded
08/09/2019	23:39:59	Internet Activity Recorded
08/09/2019	23:40:02	Internet Activity Recorded
08/09/2019	23:42:16	Internet Activity Recorded
08/09/2019	23:43:30	Internet Activity Recorded
08/09/2019	23:44:19	Internet Activity Recorded
08/09/2019	23:46:03	Internet Activity Recorded
08/09/2019	23:46:03	Internet Activity Recorded
08/09/2019	23:56:35	Internet Activity Recorded
08/09/2019	23:57:26	Internet Activity Recorded
08/09/2019	23:59:45	Internet Activity Recorded
08/09/2019	23:59:48	Internet Activity Recorded
08/10/2019	00:02:02	Internet Activity Recorded
08/10/2019	00:03:08	Internet Explorer (iexplorer.exe) is launched.
08/10/2019	00:05:03	Screen Pass is Executed by System/User - Computer System is Locked
08/10/2019	14:04:11	User BOP55722 (Robert Adams) Successfully Logged onto the System

NO USER ACTIVITY on 08/10/2019 at 00:05:03 to 08/10/2019 at 14:04:11

Perform Timeline Analysis for User Activity on the System for JP1572JE36LSNK.E01

NO USER COMPUTER USAGE BETWEEN 08/08/2019 AT 08:26:59 AND 08/10/2019 AT 08:09:24

08/08/2019 07:50:31 User BOP19020 Successfully Unlocked the System for the last time
08/08/2019 08:26:59 Screen Pass is Executed by System/User - Computer System is Locked

Identified user for 08/08/2019:

User: [REDACTED]
Username: BOP19020
SID: S-1-5-21-4149918864-1167637649-3318576334-1026

08/10/2019 08:09:24 User BOP19502 Successfully Unlocked the System

Identified user for 08/10/2019:

User: [REDACTED]
Username: BOP19502
SID: S-1-5-21-4149918864-1167637649-3318576334-1040

Preliminary Spreadsheet Generated for Timeline

Search AXIOM for Keywords

Jeffrey Edward Epstein
Jeffery
Edward
Epstein
76318-054
Reyes

Search Complete

Review Search Hits

Bookmarked One Documents for Search Term Reyes on Z6E8KD3N.E01

Bookmarked Four Documents for Search Term Reyes on JP1572JE36LSNK.E01

No Document or Communication Hits for Epstein on both Devices.

No work type documents being accessed/edited (PDF, RTF, DOC, DOCX, XLS, XLSX, WPD) around notable time for both devices.

██████ did not identify any communication on the devices regarding inmates Reyes or Epstein. BOP uses GroupWise for email communication, which does not cache email locally to BOP systems. Emails can be requested from BOP for analysis.

Forensic Analysis Complete

Begin Report of Forensic Examination (ROFE)