2019-010614 (LIMA 0384) – Forensic Notes – LITS Leonard

Forensic Request for Examination of Two Desktops from Bureau of Prisons (BOPs)

Desktops seized by SA [redacted] at MCC

Desktops collected by ASAC [redacted] and transported to the Forensic Laboratory in Crystal City, VA.

ASAC [redacted] Forensically Imaged the two Desktops

All imaging information has been loaded to LIMA Case #0384 by ASAC [redacted]

Images of Hard Drives copied to Apricorn Hard Drive SN: 101300010379 by ASAC [redacted]

Apricorn Hard Drive sent to LITS Leonard in Dallas, TX by ASAC [redacted]

FedEx Tracking # 775965711635

Hard Drive delivered to Dallas Field Office

Images copied to Forensic Workstation (X26747)

Image Information:

Z6E8K1EV.E01 -Seagate Z6E8K1EV from 0214 207270

-SHA1: 465c7bf5f62aebb6c98ecfc60534110f56274c25

-MD5 : 13e7ad6132719bae78d849e3fb914cc2

Z6E8M349.E01 -Seagate Z6E8M349 from 0214 207268

-SHA1: 465c7bf5f62aebb6c98ecfc60534110f56274c25

-MD5 : 13e7ad6132719bae78d849e3fb914cc2

Search Authority is Administrative

Case Created in EnCase 8.07.00.93

Images added to EnCase

Images Verified Successfully

Z6E8M349 - Completely Verified, 0 Errors

Acquisition MD5:	13e7ad6132719bae78d849e3fb914cc2
Verification MD5:	13e7ad6132719bae78d849e3fb914cc2

Acquisition SHA1:	465c7bf5f62aebb6c98ecfc60534110f56274c25
Verification SHA1:	465c7bf5f62aebb6c98ecfc60534110f56274c25

Z6E8K1EV - Completely Verified, 0 Errors

Acquisition MD5:	48f956e5ddab702d48177534ec96d026
Verification MD5:	48f956e5ddab702d48177534ec96d026
Acquisition SHA1:	be9791bce5978ccdf3111a54eac84606739c0424
Verification SHA1:	be9791bce5978ccdf3111a54eac84606739c0424

Run Timezone EnScript (Timezone Info Prior to Processing (V1.1).EnScript) in EnCase

Z6E8K1EV:	Eastern Standard Time
Z6E8M349:	Eastern Standard Time

Timezone changed for Z6E8K1EV and Z6E8M349 in EnCase

Z6E8M349 – Export Event Logs – Exported Successfully

Z6E8K1EV – Export Event Logs – Exported Successfully

Z6E8M349 – Export Windows Search Database – Exported Successfully

Z6E8K1EV – Export Windows Search Database – Exported Successfully

Process Z6E8M349 and Z6E8K1EV for System Info Parser

Z6E8M349 Completed Successfully

Z6E8K1EV Completed Successfully

Exported BOP Users for Z6E8M349 into Excel spreadsheet

Exported BOP Users for Z6E8K1EV into Excel spreadsheet

Z6E8M349 System Information:

Product Name	Windows 7 Professional
Current Version	6.1
Current Build Number	7601
Registered Owner	Federal Bureau of Prisons

```
        Registered Organization     U.S. Department of Justice

        Install Date                Tue, 02 Jun 2015 21:26:39 GMT

        Shutdown Time               Mon, 05 Aug 2019 16:36:42 GMT

Z6E8K1EV System Information:

        Product Name                Windows 7 Professional

        Current Version             6.1

        Current Build Number        7601

        Registered Owner            Federal Bureau of Prisons

        Registered Organization     U.S. Department of Justice

        Install Date                Thu, 14 Jun 2018 12:19:30 GMT

        Shutdown Time               Sat, 10 Aug 2019 19:16:12 GMT

Bookmark System Information for Z6E8M349

Bookmark Time Zone Information for Z6E8M349

Bookmark User Accounts for Z6E8M349

Bookmark Network Information for Z6E8M349

Bookmark USB Devices for Z6E8M349

Bookmark System Information for Z6E8K1EV

Bookmark Time Zone Information for Z6E8K1EV

Bookmark User Accounts for Z6E8K1EV

Bookmark Network Information for Z6E8K1EV

Process Z6E8K1EV for Windows Event Log Parser

        Completed Successfully

Process Z6E8M349 Windows Event Log Parser

        Completed Successfully
```

Process Z6E8K1EV for Windows Artifact Parser

Completed Successfully

Process Z6E8M349 Windows Artifact Parser

Completed Successfully

Z6E8M349 - Mount File Structure for Software Registry

Warning Banner Present in Registry

REGISTRY HIVE\Microsoft\Windows\Current Version\Policies\System\

Warning Banner Bookmarked

Z6E8K1EV - Mount File Structure for Software Registry

Warning Banner Present in Registry

REGISTRY HIVE\Microsoft\Windows\Current Version\Policies\System\

Warning Banner Bookmarked

Use Access Data Forensic Toolkit (FTK) 7.1.0.290 to check for Volume Shadow Copies:

Z6E8M349 – No Restore Points/Volume Shadows

Z6E8K1EV – No Restore Points/Volume Shadows

Use Z6E8K1EV System Event Log to establish baseline of Login/Logoff activity using the Customer Experience Improvement Program. This can later be verified against the Security Event Log.

```
Logon/Logoff Information for Z6E8K1EV from System Event Log
------------------------------------
Log Name:       System
Source:         Microsoft-Windows-Winlogon
Date:           8/8/2019 6:54:29 PM
Event ID:       7001
Task Category:  (1101)
Level:          Information
Computer:       SHU-0214207270.BOP.GOV
Description:    User Logon Notification for Customer Experience Improvement Program
SID             S-1-5-21-3548300276-3289552418-2794689317-1126
User:           Tova Noel
------------------------------------
```

```
Log Name:       System
Source:         Microsoft-Windows-Winlogon
Date:           8/9/2019 12:15:31 AM
Event ID:       7002
Task Category:  (1102)
Level:          Information
Computer:       SHU-0214207270.BOP.GOV
Description:    User Logoff Notification for Customer Experience Improvement Program
SID:            S-1-5-21-3548300276-3289552418-2794689317-1126
User:           Tova Noel
------------------------------------
Log Name:       System
Source:         Microsoft-Windows-Winlogon
Date:           8/9/2019 12:31:49 AM
Event ID:       7001
Task Category:  (1101)
Level:          Information
Computer:       SHU-0214207270.BOP.GOV
Description:    User Logon Notification for Customer Experience Improvement Program
SID:            S-1-5-21-3548300276-3289552418-2794689317-1062
User:           Thomas, Michael
------------------------------------
Log Name:       System
Source:         Microsoft-Windows-Winlogon
Date:           8/9/2019 6:29:36 AM
Event ID:       7002
Task Category:  (1102)
Level:          Information
Computer:       SHU-0214207270.BOP.GOV
Description:    User Logoff Notification for Customer Experience Improvement Program
SID:            S-1-5-21-3548300276-3289552418-2794689317-1062
User:           Thomas, Michael
------------------------------------
Log Name:       System
Source:         Microsoft-Windows-Winlogon
Date:           8/9/2019 6:30:24 AM
Event ID:       7001
Task Category:  (1101)
Level:          Information
Computer:       SHU-0214207270.BOP.GOV
Description:    User Logon Notification for Customer Experience Improvement Program
SID:            S-1-5-21-3548300276-3289552418-2794689317-1015
User:           [redacted]
------------------------------------
Log Name:       System
Source:         Microsoft-Windows-Winlogon
Date:           8/9/2019 10:51:49 AM
Event ID:       7002
```

```
Task Category:  (1102)
Level:          Information
Computer:       SHU-0214207270.BOP.GOV
Description:    User Logoff Notification for Customer Experience Improvement Program
SID:            S-1-5-21-3548300276-3289552418-2794689317-1015
User:           [redacted]
------------------------------------
Log Name:       System
Source:         Microsoft-Windows-Winlogon
Date:           8/9/2019 10:53:13 AM
Event ID:       7001
Task Category:  (1101)
Level:          Information
Computer:       SHU-0214207270.BOP.GOV
Description:    User Logon Notification for Customer Experience Improvement Program
SID:            S-1-5-21-3548300276-3289552418-2794689317-1033
User:           [redacted]
------------------------------------
Log Name:       System
Source:         Microsoft-Windows-Winlogon
Date:           8/9/2019 4:01:50 PM
Event ID:       7002
Task Category:  (1102)
Level:          Information
Computer:       SHU-0214207270.BOP.GOV
Description:    User Logoff Notification for Customer Experience Improvement Program
SID:            S-1-5-21-3548300276-3289552418-2794689317-1033
User:           [redacted]
------------------------------------
Log Name:       System
Source:         Microsoft-Windows-Winlogon
Date:           8/9/2019 4:29:54 PM
Event ID:       7001
Task Category:  (1101)
Level:          Information
Computer:       SHU-0214207270.BOP.GOV
Description:    User Logon Notification for Customer Experience Improvement Program
SID:            S-1-5-21-3548300276-3289552418-2794689317-1017
User:           [redacted]
------------------------------------
Log Name:       System
Source:         Microsoft-Windows-Winlogon
Date:           8/9/2019 4:57:41 PM
Event ID:       7002
Task Category:  (1102)
Level:          Information
Computer:       SHU-0214207270.BOP.GOV
Description:    User Logoff Notification for Customer Experience Improvement Program
```

```
SID:             S-1-5-21-3548300276-3289552418-2794689317-1017
User:            [redacted]
------------------------------------
Log Name:        System
Source:          Microsoft-Windows-Winlogon
Date:            8/9/2019 4:58:42 PM
Event ID:        7001
Task Category:   (1101)
Level:           Information
Computer:        SHU-0214207270.BOP.GOV
Description:     User Logon Notification for Customer Experience Improvement Program
SID:             S-1-5-21-3548300276-3289552418-2794689317-1126
User:            Tova Noel
------------------------------------
Log Name:        System
Source:          Microsoft-Windows-Winlogon
Date:            8/9/2019 5:06:12 PM
Event ID:        7002
Task Category:   (1102)
Level:           Information
Computer:        SHU-0214207270.BOP.GOV
Description:     User Logoff Notification for Customer Experience Improvement Program
SID:             S-1-5-21-3548300276-3289552418-2794689317-1126
User:            Tova Noel
------------------------------------
Log Name:        System
Source:          Microsoft-Windows-Winlogon
Date:            8/9/2019 5:08:46 PM
Event ID:        7001
Task Category:   (1101)
Level:           Information
Computer:        SHU-0214207270.BOP.GOV
Description:     User Logon Notification for Customer Experience Improvement Program
SID:             S-1-5-21-3548300276-3289552418-2794689317-1017
User:            [redacted]
------------------------------------
Log Name:        System
Source:          Microsoft-Windows-Winlogon
Date:            8/9/2019 5:33:13 PM
Event ID:        7001
Task Category:   (1101)
Level:           Information
Computer:        SHU-0214207270.BOP.GOV
Description:     User Logon Notification for Customer Experience Improvement Program
SID:             S-1-5-21-3548300276-3289552418-2794689317-1126
User:            Tova Noel
------------------------------------
Log Name:        System
```

```
Source:          Microsoft-Windows-Winlogon
Date:            8/9/2019 6:35:35 PM
Event ID:        7002
Task Category:   (1102)
Level:           Information
Computer:        SHU-0214207270.BOP.GOV
Description:     User Logoff Notification for Customer Experience Improvement Program
SID:             S-1-5-21-3548300276-3289552418-2794689317-1126
User:            Tova Noel
-----------------------------------
Log Name:        System
Source:          Microsoft-Windows-Winlogon
Date:            8/9/2019 6:36:27 PM
Event ID:        7001
Task Category:   (1101)
Level:           Information
Computer:        SHU-0214207270.BOP.GOV
Description:     User Logon Notification for Customer Experience Improvement Program
SID:             S-1-5-21-3548300276-3289552418-2794689317-1017
User:            [redacted]
-----------------------------------
Log Name:        System
Source:          Microsoft-Windows-Winlogon
Date:            8/9/2019 6:52:36 PM
Event ID:        7002
Task Category:   (1102)
Level:           Information
Computer:        SHU-0214207270.BOP.GOV
Description:     User Logoff Notification for Customer Experience Improvement Program
SID:             S-1-5-21-3548300276-3289552418-2794689317-1017
User:            [redacted]
-----------------------------------
Log Name:        System
Source:          Microsoft-Windows-Winlogon
Date:            8/9/2019 6:53:51 PM
Event ID:        7001
Task Category:   (1101)
User:            SYSTEM
Computer:        SHU-0214207270.BOP.GOV
Description:     User Logon Notification for Customer Experience Improvement Program
SID:             S-1-5-21-3548300276-3289552418-2794689317-1126
User:            Tova Noel
-----------------------------------
Log Name:        System
Source:          Microsoft-Windows-Winlogon
Date:            8/9/2019 8:29:29 PM
Event ID:        7002
Task Category:   (1102)
```

```
Level:          Information
Computer:       SHU-0214207270.BOP.GOV
Description:    User Logoff Notification for Customer Experience Improvement Program
SID:            S-1-5-21-3548300276-3289552418-2794689317-1126
User:           Tova Noel
------------------------------------
Log Name:       System
Source:         Microsoft-Windows-Winlogon
Date:           8/9/2019 8:32:44 PM
Event ID:       7001
Task Category:  (1101)
Level:          Information
Computer:       SHU-0214207270.BOP.GOV
Description:    User Logon Notification for Customer Experience Improvement Program
SID:            S-1-5-21-3548300276-3289552418-2794689317-1126
User:           Tova Noel
------------------------------------
Log Name:       System
Source:         Microsoft-Windows-Winlogon
Date:           8/9/2019 9:28:15 PM
Event ID:       7002
Task Category:  (1102)
Level:          Information
Computer:       SHU-0214207270.BOP.GOV
Description:    User Logoff Notification for Customer Experience Improvement Program
SID:            S-1-5-21-3548300276-3289552418-2794689317-1126
User:           Tova Noel
------------------------------------
Log Name:       System
Source:         Microsoft-Windows-Winlogon
Date:           8/9/2019 9:29:37 PM
Event ID:       7001
Task Category:  (1101)
Level:          Information
Computer:       SHU-0214207270.BOP.GOV
Description:    User Logon Notification for Customer Experience Improvement Program
SID:            S-1-5-21-3548300276-3289552418-2794689317-1017
User:           [redacted]
------------------------------------
Log Name:       System
Source:         Microsoft-Windows-Winlogon
Date:           8/9/2019 11:38:30 PM
Event ID:       7002
Task Category:  (1102)
Level:          Information
Computer:       SHU-0214207270.BOP.GOV
Description:    User Logoff Notification for Customer Experience Improvement Program
SID:            S-1-5-21-3548300276-3289552418-2794689317-1017
```

```
User:            [redacted]
------------------------------------
Log Name:        System
Source:          Microsoft-Windows-Winlogon
Date:            8/9/2019 11:40:28 PM
Event ID:        7001
Task Category:   (1101)
Level:           Information
Computer:        SHU-0214207270.BOP.GOV
Description:     User Logon Notification for Customer Experience Improvement Program
SID:             S-1-5-21-3548300276-3289552418-2794689317-1126
User:            Tova Noel
------------------------------------
Log Name:        System
Source:          Microsoft-Windows-Winlogon
Date:            8/10/2019 10:31:40 AM
Event ID:        7002
Task Category:   (1102)
Level:           Information
Computer:        SHU-0214207270.BOP.GOV
Description:     User Logoff Notification for Customer Experience Improvement Program
SID:             S-1-5-21-3548300276-3289552418-2794689317-1126
User:            Tova Noel
------------------------------------
Log Name:        System
Source:          Microsoft-Windows-Winlogon
Date:            8/10/2019 1:25:59 PM
Event ID:        7001
Task Category:   (1101)
Level:           Information
Computer:        SHU-0214207270.BOP.GOV
Description:     User Logon Notification for Customer Experience Improvement Program
SID:             S-1-5-21-3548300276-3289552418-2794689317-1018
User:            [redacted]
------------------------------------
```

Use Z6E8M349 System Event Log to establish baseline of Login/Logoff activity using the Customer Experience Improvement Program. This can later be verified against the Security Event Log.

Logon/Logoff Information for Z6E8M349 from System Event Log

```
------------------------------------
Log Name:        System
Source:          Microsoft-Windows-Winlogon
Date:            8/8/2019 3:59:37 PM
Event ID:        7001
Task Category:   (1101)
Level:           Information
```

```
Computer:        SHU-0214207268.BOP.GOV
Description:     User Logon Notification for Customer Experience Improvement Program
SID:             S-1-5-21-1823249720-3210992811-1527010081-1061
User:            [redacted]
------------------------------------
Log Name:        System
Source:          Microsoft-Windows-Winlogon
Date:            8/9/2019 12:11:23 AM
Event ID:        7002
Task Category:   (1102)
Level:           Information
Computer:        SHU-0214207268.BOP.GOV
Description:     User Logoff Notification for Customer Experience Improvement Program
SID:             S-1-5-21-1823249720-3210992811-1527010081-1061
User:            [redacted]
------------------------------------
Log Name:        System
Source:          Microsoft-Windows-Winlogon
Date:            8/9/2019 12:45:04 AM
Event ID:        7001
Task Category:   (1101)
Level:           Information
Computer:        SHU-0214207268.BOP.GOV
Description:     User Logon Notification for Customer Experience Improvement Program
SID:             S-1-5-21-1823249720-3210992811-1527010081-1244
User:            [redacted]
------------------------------------
Log Name:        System
Source:          Microsoft-Windows-Winlogon
Date:            8/9/2019 6:15:27 AM
Event ID:        7002
Task Category:   (1102)
Level:           Information
Computer:        SHU-0214207268.BOP.GOV
Description:     User Logoff Notification for Customer Experience Improvement Program
SID:             S-1-5-21-1823249720-3210992811-1527010081-1244
User:            [redacted]
------------------------------------
Log Name:        System
Source:          Microsoft-Windows-Winlogon
Date:            8/9/2019 6:17:25 AM
Event ID:        7001
Task Category:   (1101)
Level:           Information
Computer:        SHU-0214207268.BOP.GOV
Description:     User Logon Notification for Customer Experience Improvement Program
SID:             S-1-5-21-1823249720-3210992811-1527010081-1078
User:            [redacted]
```

```
------------------------------------
Log Name:       System
Source:         Microsoft-Windows-Winlogon
Date:           8/9/2019 12:14:01 PM
Event ID:       7002
Task Category:  (1102)
Level:          Information
Computer:       SHU-0214207268.BOP.GOV
Description:    User Logoff Notification for Customer Experience Improvement Program
SID:            S-1-5-21-1823249720-3210992811-1527010081-1078
User:           [redacted]
------------------------------------
Log Name:       System
Source:         Microsoft-Windows-Winlogon
Date:           8/9/2019 12:31:14 PM
Event ID:       7001
Task Category:  (1101)
Level:          Information
Computer:       SHU-0214207268.BOP.GOV
Description:    User Logon Notification for Customer Experience Improvement Program
SID:            S-1-5-21-1823249720-3210992811-1527010081-1078
User:           [redacted]
------------------------------------
Log Name:       System
Source:         Microsoft-Windows-Winlogon
Date:           8/9/2019 3:08:04 PM
Event ID:       7002
Task Category:  (1102)
Level:          Information
Computer:       SHU-0214207268.BOP.GOV
Description:    User Logoff Notification for Customer Experience Improvement Program
SID:            S-1-5-21-1823249720-3210992811-1527010081-1078
User:           [redacted]
------------------------------------
Log Name:       System
Source:         Microsoft-Windows-Winlogon
Date:           8/9/2019 3:12:39 PM
Event ID:       7001
Task Category:  (1101)
Level:          Information
Computer:       SHU-0214207268.BOP.GOV
Description:    User Logon Notification for Customer Experience Improvement Program
SID:            S-1-5-21-1823249720-3210992811-1527010081-1173
User:           [redacted]
------------------------------------
Log Name:       System
Source:         Microsoft-Windows-Winlogon
Date:           8/9/2019 9:37:44 PM
```

```
Event ID:       7002
Task Category:  (1102)
Level:          Information
Computer:       SHU-0214207268.BOP.GOV
Description:    User Logoff Notification for Customer Experience Improvement Program
SID:            S-1-5-21-1823249720-3210992811-1527010081-1173
User:           [redacted]
------------------------------------
Log Name:       System
Source:         Microsoft-Windows-Winlogon
Date:           8/10/2019 12:36:56 AM
Event ID:       7001
Task Category:  (1101)
Level:          Information
Computer:       SHU-0214207268.BOP.GOV
Description:    User Logon Notification for Customer Experience Improvement Program
SID:            S-1-5-21-1823249720-3210992811-1527010081-1102
User:           Thomas, Michael
------------------------------------
Log Name:       System
Source:         Microsoft-Windows-Winlogon
Date:           8/10/2019 5:14:13 AM
Event ID:       7002
Task Category:  (1102)
Level:          Information
Computer:       SHU-0214207268.BOP.GOV
Description:    User Logoff Notification for Customer Experience Improvement Program
SID:            S-1-5-21-1823249720-3210992811-1527010081-1102
User:           Thomas, Michael
------------------------------------
Log Name:       System
Source:         Microsoft-Windows-Winlogon
Date:           8/10/2019 6:03:33 AM
Event ID:       7001
Task Category:  (1101)
Level:          Information
Computer:       SHU-0214207268.BOP.GOV
Description:    User Logon Notification for Customer Experience Improvement Program
SID:            S-1-5-21-1823249720-3210992811-1527010081-1102
User:           Thomas, Michael
------------------------------------
Log Name:       System
Source:         Microsoft-Windows-Winlogon
Date:           8/10/2019 8:55:12 AM
Event ID:       7002
Task Category:  (1102)
Level:          Information
Computer:       SHU-0214207268.BOP.GOV
```

```
          Description:     User Logoff Notification for Customer Experience Improvement Program
          SID:             S-1-5-21-1823249720-3210992811-1527010081-1102
          User:            Thomas, Michael
          ------------------------------------
          Log Name:        System
          Source:          Microsoft-Windows-Winlogon
          Date:            8/10/2019 9:21:25 AM
          Event ID:        7001
          Task Category:   (1101)
          Level:           Information
          Computer:        SHU-0214207268.BOP.GOV
          Description:     User Logon Notification for Customer Experience Improvement Program
          SID:             S-1-5-21-1823249720-3210992811-1527010081-1028
          User:            [redacted]
          ------------------------------------
          Log Name:        System
          Source:          Microsoft-Windows-Winlogon
          Date:            8/10/2019 2:13:48 PM
          Event ID:        7002
          Task Category:   (1102)
          Level:           Information
          Computer:        SHU-0214207268.BOP.GOV
          Description:     User Logoff Notification for Customer Experience Improvement Program
          SID:             S-1-5-21-1823249720-3210992811-1527010081-1028
          User:            [redacted]
          ------------------------------------
          Log Name:        System
          Source:          Microsoft-Windows-Winlogon
          Date:            8/10/2019 2:15:20 PM
          Event ID:        7001
          Task Category:   (1101)
          Level:           Information
          Computer:        SHU-0214207268.BOP.GOV
          Description:     User Logon Notification for Customer Experience Improvement Program
          SID:             S-1-5-21-1823249720-3210992811-1527010081-1173
          User:            [redacted]
          ------------------------------------
------------------------------------------------------------------------
```

Z6E8M349 User Account Logged in at potential time of death is Thomas, Michael

BOP Account: bop19012   SID: S-1-5-21-1823249720-3210992811-1527010081-1102

Z6E8K1EV User Accout Logged in at potential time of death is Tova Noel

BOP Account: bop61232   SID: S-1-5-21-3548300276-3289552418-2794689317-1126

Spoke with ASAC [redacted] providing update regarding users logged in from 8/10/19 at 12:00:00 AM through the morning. Will provide similar update to case agent.

Use Magnet AXIOM Process 3.4.1.15164

- Add the Z6E8M349 image and Z6E8K1EV image into AXIOM Process
- Z6E8M349 contains three partitions:
  - Partition 1 (EXT-family, 165.85MB)
  - Partition 2 (Microsoft NTFS, 95MB) – System Reserved
  - Partition 3 (Microsoft NTFS, 465.51 GB)
  - Unpartitioned Space
- Z6E8K1EV contains one partition:
  - Partition 1 (Microsoft NTFS, 465.76)
  - Unpartitioned Space
- Search archives and mobile backups is turned on
- Calculate hash values is turned off to speed up processing time.
- Processing Started
- Z6E8M349 Processed Successfully
- Z6E8K1EV Experienced a Timeout Error during Processing
  - Stuck at 15.5% processing on All Files and Folders for 4 hours
  - Data Processor #9 timeout info:
    - Current search item: Data Processor 9: Searching [ROOT]\Windows\MEMORY.DMP at offset 54525952
    - See TimeoutInfo 8-14 Log for additional information
      - Attached to Notes
- Magnet AXIOM Processing Canceled for Z6E8K1EV
- Magnet AXIOM Closed

Magnet AXIOM Examine 3.4.1.15164 Launched

2019-010614 Case Loaded

Continuing processing for Z6E8K1EV canceled

Processing Completed

Will need to run AXIOM Process on Z6E8K1EV in a separate case.

AXIOM Examine checking Indices

AXIOM Examine is locked up and not responding

AXIOM Examine is closed and re-launched

2019-010614 Case is loaded

AXIOM Examine checking Indices

AXIOM Examine is locked up and not responding

AXIOM Processing will be performed again for both images.

Continue Examination in EnCase 8.07.00.93

Note: Full EnCase Processing has not been completed at this time.

Process Recover Folders for Z6E8M349

Completed Successfully

Process Recover Folders for Z6E8K1EV

Completed Successfully

Export Logical Evidence File of Michael Thomas user's profile (bop19012) on Z6E8M349

Named BOP19012.L01

Export Logical Evidence File of Tova Noel user's profile (bop61232) on Z6E8K1EV

Named BOP61232.L01

Email used by BOP is called GroupWise

GroupWise Email can be cached locally to a system if configured to do so

Path for cached email \USERACCOUT\AppData\Local\Novell\Groupwise\USERACCOUNT

Checked GroupWise Email for Michael Thomas (bop19012) on Z6E8M349

No Cached Email

Checked GroupWise Email for Tova Noel (bop61232) on Z6E8K1EV

No Cached Email

One GWErrorLog.txt – Attachment Error on 6/26/2019

Use Magnet AXIOM Process 3.4.1.15164

Add the BOP19012 Logical Evidence File to AXIOM Process

Search archives and mobile backups is turned on

Calculate hash values is turned off to speed up processing time.

Uncheck "Find more artifacts" to speed up processing time.

Attempts to locate and parse SQLite Databases

Processing Started

Processing Completed Successfully

```
Summary:
========
Start Time: Aug 14, 2019 12:27:09
End Time: Aug 14, 2019 12:28:38
Search Duration: 00:01:18
Indexing Duration: 00:00:00
Search Outcome: Success

Final results of search:
========================
AutoRun Items: 1 items
Carved Archives (content not searched): 96 items
Carved Audio: 1 items
Classifieds URLs: 171 items
Cloud Services URLs: 4 items
Edge/Internet Explorer 10-11 Content: 20373 items
Edge/Internet Explorer 10-11 Cookies: 514 items
Edge/Internet Explorer 10-11 Daily/Weekly History: 846 items
Edge/Internet Explorer 10-11 Dependency Entries: 15 items
```

Edge/Internet Explorer 10-11 Main History: 3138 items
Facebook URLs: 26 items
File System Information: 1 items
Flash Cookies: 17 items
Google Analytics First Visit Cookies: 14 items
Google Analytics First Visit Cookies Carved: 14 items
Google Analytics Referral Cookies: 14 items
Google Analytics Referral Cookies Carved: 13 items
Google Analytics Session Cookies: 4 items
Google Analytics Session Cookies Carved: 4 items
Google Searches: 8 items
Identifiers: 14 items
Internet Explorer Cookies: 1761 items
Internet Explorer Favorites: 17 items
Internet Explorer Typed URLs: 8 items
Jump Lists: 81 items
Keyword Searches: 4 items
LNK Files: 526 items
MRU Folder Access: 1 items
MRU Opened/Saved Files: 4 items
MRU Recent Files & Folders: 90 items
MUICache: 92 items
Network Share Information: 3 items
Parsed Search Queries: 102 items
PDF Documents: 5 items
Pictures: 5342 items
Potential Browser Activity: 82 items
Prefetch Files - Windows XP/Vista/7: 7 items
RTF Documents: 3 items
Shellbags: 95 items
Social Media URLs: 18 items
Startup Items: 1 items
Tax Site URLs: 1 items
Text Documents: 628 items
UserAssist: 58 items
Videos: 34 items
VLC Recently Played Files: 3 items
WebKit Browser Web History (Carved): 3 items
Word Documents: 22 items

Add the BOP61232 Logical Evidence File to AXIOM Process

Search archives and mobile backups is turned on

Calculate hash values is turned off to speed up processing time.

Uncheck “Find more artifacts” to speed up processing time.

```
        Attempts to locate and parse SQLite Databases

Processing Started

Processing Completed Successfully

        Summary:
        ========
        Start Time: Aug 14, 2019 12:38:52
        End Time: Aug 14, 2019 12:40:14
        Search Duration: 00:01:08
        Indexing Duration: 00:00:00
        Search Outcome: Success

        Final results of search:
        ========================
        Audio: 4 items
        AutoRun Items: 1 items
        Carved Archives (content not searched): 58 items
        Carved Audio: 50 items
        Classifieds URLs: 671 items
        Edge/Internet Explorer 10-11 Content: 17682 items
        Edge/Internet Explorer 10-11 Cookies: 468 items
        Edge/Internet Explorer 10-11 Daily/Weekly History: 2172 items
        Edge/Internet Explorer 10-11 Dependency Entries: 57 items
        Edge/Internet Explorer 10-11 Main History: 4602 items
        Facebook URLs: 5 items
        File System Information: 1 items
        Flash Cookies: 6 items
        Google Analytics First Visit Cookies: 11 items
        Google Analytics First Visit Cookies Carved: 11 items
        Google Analytics Referral Cookies: 11 items
        Google Analytics Referral Cookies Carved: 10 items
        Google Analytics Session Cookies: 6 items
        Google Analytics Session Cookies Carved: 6 items
        Google Maps: 7 items
        Google Searches: 446 items
        Identifiers: 13 items
        Internet Explorer Cookies: 1667 items
        Internet Explorer Favorites: 17 items
        Internet Explorer Typed URLs: 9 items
        Jump Lists: 53 items
        LNK Files: 112 items
        MRU Folder Access: 4 items
        MRU Opened/Saved Files: 16 items
        MRU Recent Files & Folders: 34 items
        MUICache: 62 items
        Network Share Information: 3 items
```

Parsed Search Queries: 84 items
PDF Documents: 10 items
Pictures: 3551 items
Potential Browser Activity: 172 items
RTF Documents: 1 items
Shellbags: 91 items
Social Media URLs: 14 items
Startup Items: 1 items
Tax Site URLs: 1 items
Text Documents: 588 items
UserAssist: 40 items
Videos: 8 items
WebKit Browser Web History (Carved): 1 items
Word Documents: 13 items

Continue Examination in EnCase 8.07.00.93

Export RECENT Folder for Michael Thomas (bop19012) on Z6E8M349

Review JumpLists in [redacted] JumpList Explorer v0.5.0.0

Export RECENT Folder for Tova Noel (bop61232) on Z6E8K1EV

Review JumpLists in [redacted] JumpList Explorer v0.5.0.0

Process File Signature Analysis for Z6E8M349

Completed Successfully

Process File Signature Analysis on Z6E8K1EV

Completed Successfully

Process Protected File Analysis for Z6E8M349

Completed Successfully

Process Protected File Analysis for Z6E8K1EV

Completed Successfully

Review the Michael Thomas user profile (bop19012) on Z6E8M349

Low Activity for the user during the time frame on Z6E8M349

"SHU 30 CHECK SHEET (CONDENSED)_1.docx" in \Documents\Groupwise

File Created 8/10/19 12:39:31   Last Modified 8/10/19 12:43:33

File is a Check Sheet for each 30 minutes, but is not filled out.

Only File with Time Stamp Information on the day of question.

"~$U 30 CHECK SHEET (CONDENSED)_1.docx" in \Documents\Groupwise

File Created 8/10/19 12:40:28   Last Modified 8/10/19 12:40:28

Tilde is commonly associated as backup files of a file that was opened or is still currently opened.

Possibly indicates the file was saved to the Groupwise location and opened, but never populated.

Review the Tova Noel profile (bop61232) on Z6E8K1EV

Low Activity for the user during time frame on Z6E8K1EV

No Work Files with Time Stamp Information on the day of question within profile.

Process Thumbnail Creation for Z6E8M349

Completed Successfully

Process Thumbnail Creation for Z6E8K1EV

Completed Successfully

Recycle Bin for S-1-5-21-1823249720-3210992811-1527010081-1102 on Z6E8M349 examined

Only contains DESKTOP. FILE – System File

No User Files

Recycle Bin for SID: S-1-5-21-3548300276-3289552418-2794689317-1126 on Z6E8K1EV examined

Only contains DESKTOP. FILE – System File

No User Files

Use Magnet AXIOM Examine 3.4.1.15164

Load "AXIOM - BOP19012 - Z6E8M349" Case for BOP19012 User Profile

Time Zone settings changed to EST (with Daylight Savings)

Build Timeline

Completed Successfully

Build Connections

Completed Successfully

Load "AXIOM - BOP61232 - Z6E8K1EV" Case for BOP61232 User Profile

Time Zone settings changed to EST (with Daylight Savings)

Build Timeline

Completed Successfully

Build Connections

Completed Successfully

Both Physical Images of the BOP desktops will be processed through AXIOM. The processing of the user profiles is to examine user activity on the computers while the lengthy processing is conducted for the hard drive images.

Review "AXIOM - BOP19012 - Z6E8M349" Case in Magnet AXIOM Examine 3.4.1.15164

Network Usage with BOP Applications

http://sallyport.bop.gov/inst/nym/corrsvc/docs/Daily%20Fire%20&%20Security%20Form.pdf

file:///K:/BOPAPPS/Roster/Ver3.1/Roster.accde

file:///I:/GROUPS/SHAREDOC/SHU PAPERWORK, LOCATOR, HARDCOPY/1 - SHU LOCATOR 2019(HARDCOPY).docx

Google Search for "suzuki gsx-r 1000 motorcycle for sale" 8/10/19 01:00:52

Google Search for "suzuki gsx-r 750 motorcycle for sale" on 8/10/19 01:00:52

Bing Search for "cycletrader" on 8/10/19 01:00:24

Bing Search for "espn" on 8/10/19 06:15:03

Internet Usage is consistent with search times

No recorded usage between 01:03:20 and 06:04:30

Edge/Internet Explorer History records File Access within Windows Explorer file:///C:/Users/bop19012/Desktop/SHU ORDERLY REQUEST 42214.rtf

8/10/2019 12:44:53 AM

Not Located on the Desktop

Potential other files accessed – will continue in depth search

Artifacts indicating that the user profile was used to watch Django Unchained 2012 DVDSCR XVI, but this took place in 5/12/2019 12:00:30 PM

Three Network Shares:

\\NYMC_APPS_SERVER\APPS

\\NYMC_GRPS_SERVER\GRPS

\\NYMC_HOME_SERVER\HOME\HOME\BOP19012

Review "AXIOM - BOP61232 - Z6E8K1EV" Case in Magnet AXIOM Examine 3.4.1.15164

Network Usage with BOP Applications

\\NYMC_APPS_SERVER\APPS\BOPAPPS\Roster\Ver3.1\Roster.accde

Google Search for "epp" on 8/10/2019 04:31:33

Google Search for "unum insurance" on 8/10/2019 04:36:00

Google Search for " usajobs" on 8/10/2019 04:39:01

Google Search for "furniture bronx ny" on 8/10/2019 04:48:23

Google Search for "ashleys furniture" on 8/10/2019 04:52:12

Google Search for "KENYATTA TAISTE" on 8/10/2019 05:38:55

Google Search for "latest on epstein in jail" on 8/10/2019 05:42:56 & 8/10/2019 05:52:29

Google Search for "latest on omar amanat" on 8/10/2019 05:53:02

Google Search for "law enforcement discounts" on 8/10/2019 06:17:23

Bing Search for "calendar 2019" on 8/10/2019 4:33:13 AM

Internet Usage: 8/10/19 03:56:00 to 8/10/19 06:19:12

Three Network Shares:

\\NYMC_APPS_SERVER\APPS

\\NYMC_GRPS_SERVER\GRPS

\\NYMC_HOME_SERVER\HOME\HOME\ BOP61232

Briefed ASAC [redacted] on preliminary findings.

Phone conference with ASAC [redacted] and Case Agent regarding preliminary findings.

Use Magnet AXIOM Process 3.4.1.15164

Add the Z6E8M349 image into AXIOM Process

Z6E8M349 contains three partitions:

Partition 1 (EXT-family, 165.85MB)

Partition 2 (Microsoft NTFS, 95MB) – System Reserved

Partition 3 (Microsoft NTFS, 465.51 GB)

Unpartitioned Space

Search archives and mobile backups is turned on

Calculate hash values is turned off to speed up processing time.

Uncheck "Find more artifacts" to speed up processing time.

Attempts to locate and parse SQLite Databases

Processing Started

Processing Completed Successfully

```
Summary:
========
Start Time: Aug 14, 2019 12:42:01
End Time: Aug 15, 2019 02:47:05
Search Duration: 14:04:51
Indexing Duration: 00:00:50
Search Outcome: Success

Final results of search:
========================
$LogFile Analysis: 17080 items
AmCache Device Containers: 39 items
```

AmCache Driver Binaries: 270 items
AmCache Driver Packages: 17 items
AmCache File Entries: 807 items
AmCache Pnp Devices: 96 items
AmCache Program Entries: 152 items
AmCache Shortcuts: 1202 items
Audio: 3352 items
AutoRun Items: 888 items
Backpage Ads: 4 items
Carved Archives (content not searched): 11656 items
Carved Audio: 2655 items
Carved Video: 1346 items
Carved WebM Video: 59 items
Classifieds URLs: 54311 items
Cloud Services URLs: 65 items
Craigslist Ads: 20 items
CSV Documents: 15 items
Dating Sites URLs: 16 items
Edge/Internet Explorer 10-11 Content: 2623231 items
Edge/Internet Explorer 10-11 Cookies: 64396 items
Edge/Internet Explorer 10-11 Daily/Weekly History: 224242 items
Edge/Internet Explorer 10-11 Dependency Entries: 4903 items
Edge/Internet Explorer 10-11 Downloads: 123 items
Edge/Internet Explorer 10-11 Main History: 340974 items
Email Attachments: 6 items
EML(X) Files: 324 items
Encrypted Files: 175 items
Encryption / Anti-forensics Tools: 7 items
Excel Documents: 126 items
Facebook Chat: 379 items
Facebook Pages: 11 items
Facebook URLs: 2475 items
File Associations: 2173 items
File System Information: 3 items
Firefox Add-ons: 1 items
Firefox Bookmarks: 13 items
Firefox Cache Records: 11312 items
Firefox Cookies: 794 items
Firefox FavIcons: 27 items
Firefox FormHistory: 8 items
Firefox Input History: 1 items
Firefox SessionStore Artifacts: 238 items
Firefox Web History: 175 items
Firefox Web Visits: 230 items
Flash Cookies: 4890 items
Gmail Webmail: 210 items
Google Analytics First Visit Cookies: 3420 items
Google Analytics First Visit Cookies Carved: 8876 items

Google Analytics Referral Cookies: 3187 items
Google Analytics Referral Cookies Carved: 7584 items
Google Analytics Session Cookies: 1816 items
Google Analytics Session Cookies Carved: 4525 items
Google Analytics URLs: 682 items
Google Analytics URLs Carved: 278 items
Google Maps: 764 items
Google Maps Queries: 247 items
Google Maps Tiles: 714 items
Google Searches: 19466 items
Google WebP Images: 37 items
Hangul Word Processor: 2 items
Identifiers: 3177 items
IE InPrivate/Recovery URLs: 18 items
Installed Microsoft Programs: 304 items
Installed Programs: 225 items
Internet Explorer Cookies: 219421 items
Internet Explorer Daily History: 2 items
Internet Explorer Favorites: 4147 items
Internet Explorer Main History: 11 items
Internet Explorer Typed URLs: 1968 items
IP Addresses - Audio/Video Calls: 1 items
Jump Lists: 14133 items
Keyword Searches: 213 items
Known DLLs: 56 items
LNK Files: 52485 items
Malware/Phishing URLs: 43 items
MRU Folder Access: 441 items
MRU Opened/Saved Files: 2441 items
MRU Recent Files & Folders: 9614 items
MUICache: 22994 items
Network Interfaces (Registry): 2 items
Network Profiles: 3 items
Network Share Information: 707 items
Operating System Information: 2 items
Parsed Search Queries: 16364 items
PDF Documents: 1895 items
Photoshop Files: 90 items
Pictures: 866412 items
Pornography URLs: 1 items
Potential Browser Activity: 66631 items
Potential Facebook Pictures: 2063 items
PowerPoint Documents: 81 items
Prefetch Files - Windows XP/Vista/7: 294 items
QuickBooks Files: 77 items
Rebuilt Webpages: 38485 items
Remote Desktop Protocol: 54 items
RTF Documents: 1150 items

Safari History: 3 items

Shellbags: 18841 items

Shipping Site URLs: 266 items

Social Media URLs: 2511 items

Startup Items: 273 items

System Services: 905 items

Tax Site URLs: 316 items

Text Documents: 86855 items

Timezone Information: 1 items

Torrent URLs: 8 items

USB Devices: 156 items

User Accounts: 278 items

UserAssist: 9903 items

Videos: 5588 items

VLC Recently Played Files: 78 items

Web Video Fragments: 32 items

WebKit Browser Web History (Carved): 250 items

Windows Event Logs: 350501 items

Windows Logon Banner: 1 items

Word Documents: 3665 items

WordPerfect Files: 12 items

Yahoo! Non-Encrypted Chat: 417 items

Use Magnet AXIOM Examine 3.4.1.15164

Load “AXIOM - Z6E8M349” Case for Z6E8M349 Image

Time Zone settings changed to EST (with Daylight Savings)

Build Timeline

Completed Successfully

Build Connections

Completed Successfully

Use Magnet AXIOM Process 3.4.1.15164

Add the Z6E8K1EV image into AXIOM Process

Z6E8K1EV contains one partition:

Partition 1 (Microsoft NTFS, 465.76)

Unpartitioned Space

Search archives and mobile backups is turned on

Calculate hash values is turned off to speed up processing time.

Uncheck “Find more artifacts” to speed up processing time.

Attempts to locate and parse SQLite Databases

Processing Started

Experienced a Timeout Error during Processing

Stuck at 15.5% processing on All Files and Folders for 3 hours

Data Processor #9 timeout info:

Current search item: Data Processor 9: Searching [ROOT]\Windows\MEMORY.DMP at offset 54525952

See TimeoutInfo 8-15 Log for additional information

Attached to Notes

Consulted with SSA [redacted] regarding Timeout Error.

SSA [redacted] noted that a logical image could be created of the user profile and windows folder for analysis

Launch EnCase 8.07.00.93 and open 2019-010614 Case

Z6E8K1EV Image opened

All Files Selected for Image

MEMORY.DMP unselected

Only BOP 19012 user checked

Program Files and Program Files (x86) unchecked

Size is over 300GBs

“ao” unchecked as it is empty

Recycle Bin not checked as user bop19012 had no files in Recycle Bin

Acquire Logical Evidence File

Set as L01 with Compression

Approximately 150GB of data

Begin Image Creation

Completed Successfully

Use Magnet AXIOM Process 3.4.1.15164

Add the Z6E8K1EV Logical image into AXIOM Process

Search archives and mobile backups is turned on

Calculate hash values is turned off to speed up processing time.

Uncheck “Find more artifacts” to speed up processing time.

Attempts to locate and parse SQLite Databases

Processing Started

Processing Completed Successfully

```
Summary:
========
Start Time: Aug 15, 2019 13:12:45
End Time: Aug 15, 2019 15:16:12
Search Duration: 02:03:15
Indexing Duration: 00:00:14
Search Outcome: Success

Final results of search:
========================
$LogFile Analysis: 16649 items
AmCache Device Containers: 23 items
AmCache Driver Binaries: 262 items
AmCache Driver Packages: 16 items
AmCache File Entries: 636 items
AmCache Pnp Devices: 95 items
AmCache Program Entries: 139 items
AmCache Shortcuts: 1118 items
Audio: 689 items
AutoRun Items: 604 items
Carved Archives (content not searched): 361 items
Carved Audio: 1063 items
Carved Video: 657 items
```

Carved WebM Video: 9 items
Classifieds URLs: 1446 items
Cloud Services URLs: 13 items
CSV Documents: 2 items
Edge/Internet Explorer 10-11 Content: 90701 items
Edge/Internet Explorer 10-11 Daily/Weekly History: 8754 items
Edge/Internet Explorer 10-11 Main History: 18062 items
Email Attachments: 2 items
EML(X) Files: 6 items
Encrypted Files: 5 items
Encryption / Anti-forensics Tools: 4 items
Excel Documents: 88 items
Facebook URLs: 89 items
File Associations: 2126 items
File System Information: 1 items
Firefox SessionStore Artifacts: 122 items
Flash Cookies: 444 items
Google Analytics First Visit Cookies Carved: 622 items
Google Analytics Referral Cookies Carved: 548 items
Google Analytics Session Cookies Carved: 344 items
Google Analytics URLs: 2 items
Google Analytics URLs Carved: 2 items
Google Maps: 16 items
Google Maps Queries: 7 items
Google Searches: 714 items
Google WebP Images: 1 items
Hangul Word Processor: 1 items
Identifiers: 893 items
Installed Microsoft Programs: 300 items
Installed Programs: 194 items
Internet Explorer Favorites: 14 items
Known DLLs: 56 items
LNK Files: 3059 items
Malware/Phishing URLs: 4 items
Network Interfaces (Registry): 2 items
Network Profiles: 3 items
Operating System Information: 2 items
Parsed Search Queries: 931 items
PDF Documents: 229 items
Photoshop Files: 23 items
Pictures: 115767 items
Pornography URLs: 1 items
Potential Browser Activity: 17325 items
PowerPoint Documents: 5 items
Prefetch Files - Windows XP/Vista/7: 361 items
Remote Desktop Protocol: 61 items
RTF Documents: 628 items
Social Media URLs: 110 items

Startup Items: 16 items
System Services: 889 items
Tax Site URLs: 7 items
Text Documents: 1872 items
Timezone Information: 1 items
USB Devices: 76 items
User Accounts: 208 items
Videos: 104 items
WebKit Browser Web History (Carved): 37 items
Windows Event Logs: 326681 items
Windows Logon Banner: 1 items
Word Documents: 2 items
Yahoo! Non-Encrypted Chat: 159 items

Use Magnet AXIOM Examine 3.4.1.15164

Load "AXIOM - Z6E8K1EV (L01)" Case for Z6E8K1EV Logical Image

Time Zone settings changed to EST (with Daylight Savings)

Build Timeline

Completed Successfully

Build Connections

Completed Successfully

Use Magnet AXIOM Process 3.4.1.15164

Add the Z6E8K1EV image into AXIOM Process

Z6E8K1EV contains one partition:

Partition 1 (Microsoft NTFS, 465.76)

Unpartitioned Space

Search archives and mobile backups is turned on

Calculate hash values is turned off to speed up processing time.

Uncheck "Find more artifacts" to speed up processing time.

Attempts to locate and parse SQLite Databases

Processing Started

Experienced a Timeout Error during Processing

Continue Running

Processing Completed, with Timeout Errors

> See TimeoutInfo 8-15 Log for additional information
>
> Attached to Notes

```
Summary:
========
Start Time: Aug 16, 2019 17:43:57
End Time: Aug 17, 2019 04:24:22
Search Duration: 10:40:13
Indexing Duration: 00:00:37
Search Outcome: Success

Final results of search:
========================
$LogFile Analysis: 16649 items
AmCache Device Containers: 23 items
AmCache Driver Binaries: 262 items
AmCache Driver Packages: 16 items
AmCache File Entries: 636 items
AmCache Pnp Devices: 95 items
AmCache Program Entries: 139 items
AmCache Shortcuts: 1118 items
Audio: 2911 items
AutoRun Items: 779 items
Carved Archives (content not searched): 7044 items
Carved Audio: 1921 items
Carved Video: 2563 items
Carved WebM Video: 22 items
Classifieds URLs: 24441 items
Cloud Services URLs: 155 items
Craigslist Ads: 5 items
CSV Documents: 7 items
Edge/Internet Explorer 10-11 Content: 1890373 items
Edge/Internet Explorer 10-11 Cookies: 31265 items
Edge/Internet Explorer 10-11 Daily/Weekly History: 134602 items
Edge/Internet Explorer 10-11 Dependency Entries: 2791 items
Edge/Internet Explorer 10-11 Downloads: 13 items
Edge/Internet Explorer 10-11 Main History: 238010 items
Email Attachments: 12 items
EML(X) Files: 72 items
```

Encrypted Files: 198 items
Encryption / Anti-forensics Tools: 7 items
Excel Documents: 127 items
Facebook Chat: 295 items
Facebook Pages: 2 items
Facebook URLs: 1148 items
File Associations: 2132 items
File System Information: 1 items
Firefox SessionStore Artifacts: 955 items
Flash Cookies: 1083 items
Google Analytics First Visit Cookies: 623 items
Google Analytics First Visit Cookies Carved: 1304 items
Google Analytics Referral Cookies: 603 items
Google Analytics Referral Cookies Carved: 1132 items
Google Analytics Session Cookies: 365 items
Google Analytics Session Cookies Carved: 721 items
Google Analytics URLs: 285 items
Google Analytics URLs Carved: 72 items
Google Maps: 711 items
Google Maps Queries: 99 items
Google Maps Tiles: 688 items
Google Searches: 14194 items
Google WebP Images: 2 items
Hangul Word Processor: 2 items
Identifiers: 2044 items
IE InPrivate/Recovery URLs: 48 items
Installed Microsoft Programs: 300 items
Installed Programs: 194 items
Internet Explorer Cookies: 104747 items
Internet Explorer Favorites: 3012 items
Internet Explorer Typed URLs: 908 items
Jump Lists: 8570 items
Keyword Searches: 100 items
Known DLLs: 56 items
LNK Files: 21371 items
Malware/Phishing URLs: 32 items
MRU Folder Access: 180 items
MRU Opened/Saved Files: 908 items
MRU Recent Files & Folders: 4676 items
MUICache: 11386 items
Network Interfaces (Registry): 2 items
Network Profiles: 3 items
Network Share Information: 520 items
Operating System Information: 2 items
Parsed Search Queries: 12515 items
PDF Documents: 917 items
Photoshop Files: 92 items
Pictures: 530872 items

Plenty of Fish: 1 items
Pornography URLs: 2 items
Potential Browser Activity: 37065 items
Potential Facebook Pictures: 2307 items
PowerPoint Documents: 17 items
Prefetch Files - Windows XP/Vista/7: 487 items
Rebuilt Webpages: 24356 items
Remote Desktop Protocol: 70 items
RTF Documents: 692 items
Safari History: 3 items
Shellbags: 15151 items
Shipping Site URLs: 892 items
Social Media URLs: 1493 items
Startup Items: 192 items
System Services: 889 items
Tax Site URLs: 607 items
Text Documents: 44382 items
Timezone Information: 1 items
USB Devices: 76 items
User Accounts: 208 items
UserAssist: 6385 items
UsnJrnl: 318579 items
Videos: 2010 items
VLC Recently Played Files: 29 items
WebKit Browser Web History (Carved): 173 items
Windows Event Logs: 326681 items
Windows Logon Banner: 1 items
Word Documents: 1314 items
WordPerfect Files: 3 items
Yahoo! Non-Encrypted Chat: 161 items

Use Magnet AXIOM Examine 3.4.1.15164

Load "AXIOM - Z6E8K1EV" Case for Z6E8K1EV Image

Time Zone settings changed to EST (with Daylight Savings)

Build Timeline

Completed Successfully

Build Connections

Completed Successfully

```
Continue Examination in EnCase 8.07.00.93
        Process Hash Analysis for Z6E8M349
                Completed Successfully
        Process Hash Analysis for Z6E8K1EV
                Completed Successfully
        Process Expand Compound Files for Z6E8M349
                Completed Successfully
        Process Expand Compound Files for Z6E8K1EV
                Completed Successfully
        Process Find Email (Defaults) for Z6E8M349
                Completed Successfully
        Process Find Email (Defaults) for Z6E8K1EV
                Completed Successfully
        Process Find Internet Artifacts for Z6E8M349
                Completed Successfully
        Process Find Internet Artifacts for Z6E8K1EV
                Completed Successfully
        Process Index Text and Metadata for Z6E8M349
                Default Language (English) Selected
                Index Slack and Unallocated Selected
                Completed Successfully
        Process Index Text and Metadata for Z6E8K1EV
                Default Language (English) Selected
                Index Slack and Unallocated Selected
                Completed Successfully
```

Use Magnet AXIOM Examine 3.4.1.15164

Load "AXIOM - Z6E8M349" Case for Z6E8M349 Image

Open Timeline

Filter Date 8/10/2019

Begin review of BOP19012 Activity

Starts at 8/10/2019 at 12:36:54 with User Login

Begin analysis and bookmarking of relevant Timeline Activity

8-10-19 1:13:49 – Screen Pass (3rd Party Time Comp Lock)

8-10-19 6:02:13 – Failed Login

8-10-19 6:04:06 – Continue and lookup nearby NDPS

5726 System Artifacts Bookmarked

Use Magnet AXIOM Examine 3.4.1.15164

Load "AXIOM - Z6E8K1EV" Case for Z6E8K1EV Image

Open Timeline

Filter Date 8/10/2019

Begin Review of BOP61232

Starts at 8/9/2019 at 23:40:27 with User Login

Begin analysis and bookmarking of relevant Timeline Activity

8-10-19 12:10:30 – Screen Pass (Computer Lock)

8-10-19 06:12:26 – Screen Pass

24,586 Artifacts Bookmarked

Screen Pass 64 v6.7.1

Begin building time line for Z6E8K1EV.

Preliminary Timeline Established

90 Events Recorded

Begin building time line for Z6E8M349.

Preliminary Timeline Established

51 Events Recorded

TO DO

- Check System for Computer Screen Lock Settings
- Check System for IE Homepage Settings

Start Report of Forensic Examination

Two additional desktops received by Crystal City Forensic Laboratory for Imaging

Devices imaged by ASAC [redacted]

EnCase Forensic Images copied to Apricorn Encrypted Hard Drive

Apricorn Hard Drive handed to LITS Leonard for transport back to Dallas

Working copies of EnCase Forensic Images made in Dallas

Image Information:

```
        Z6E8KD3N.E01  - Hitachi HDS721050CLA662 from 0214 207266

                      -SHA1: 3ac4c0fa2b1cb97020e22bc3966d4b3609c89d57

                      -MD5 : 629694386155e0f49e7a8c0da0da2840

        JP1572JE36LSNK.E01     -Seagate ST500DM002 from 0214 107384

                      -SHA1: 0d78251b33302e327c56c1ef28e9ccc8f353bd46

                      -MD5 : 0dd9c2ad818c4a5a58bab2f78d57f2d7
```

```
Hashes of working copies of EnCase Forensic Images verified successfully.

Images added to EnCase Case# 2019-010614

        Images Verified Successfully

                Z6E8KD3N - Completely Verified, 0 Errors

                        Acquisition MD5:        629694386155e0f49e7a8c0da0da2840

                        Verification MD5:       629694386155e0f49e7a8c0da0da2840

                        Acquisition SHA1:       3ac4c0fa2b1cb97020e22bc3966d4b3609c89d57

                        Verification SHA1:      3ac4c0fa2b1cb97020e22bc3966d4b3609c89d57

                JP1572JE36LSNK - Completely Verified, 0 Errors

                        Acquisition MD5:        0dd9c2ad818c4a5a58bab2f78d57f2d7

                        Verification MD5:       0dd9c2ad818c4a5a58bab2f78d57f2d7

                        Acquisition SHA1:       0d78251b33302e327c56c1ef28e9ccc8f353bd46

                        Verification SHA1:      0d78251b33302e327c56c1ef28e9ccc8f353bd46

        Run Timezone EnScript (Timezone Info Prior to Processing (V1.1).EnScript) in EnCase

                Z6E8KD3N:               Eastern Standard Time

                JP1572JE36LSNK:         Eastern Standard Time

        Timezone changed for Z6E8KD3N and JP1572JE36LSNK in EnCase

        Process Z6E8KD3N and JP1572JE36LSNK for System Info Parser

                Z6E8KD3N Completed Successfully

                JP1572JE36LSNK Completed Successfully

        Process Recover Folders for Z6E8KD3N

                Completed Successfully

        Process Recover Folders for JP1572JE36LSNK

                Completed Successfully

        Process File Signature Analysis for Z6E8KD3N
```

Completed Successfully

Process File Signature Analysis for JP1572JE36LSNK

Completed Successfully

Process Protected File Analysis for Z6E8KD3N

Completed Successfully

Process Protected File Analysis for JP1572JE36LSNK

Completed Successfully

Process Thumbnail Creation for Z6E8KD3N

Completed Successfully

Process Thumbnail Creation for JP1572JE36LSNK

Completed Successfully

Process Hash Analysis for Z6E8KD3N

Job Failed: Error Processing

Re-run Processing

Completed Successfully

Process Hash Analysis for JP1572JE36LSNK

Completed Successfully

Process Expand Compound Files for Z6E8KD3N

Completed Successfully

Process Expand Compound Files for JP1572JE36LSNK

Job Failed: Error Processing

Re-Run Processing

Completed Successfully

Process Find Email (Defaults) for Z6E8KD3N

Completed Successfully

Process Find Email (Defaults) for JP1572JE36LSNK

Completed Successfully

Process Find Internet Artifacts for Z6E8KD3N

Completed Successfully

Process Find Internet Artifacts for JP1572JE36LSNK

Completed Successfully

Process Index Text and Metadata for Z6E8KD3N

Default Language (English) Selected

Index Slack and Unallocated Selected

Completed Successfully

Process Index Text and Metadata for JP1572JE36LSNK

Default Language (English) Selected

Index Slack and Unallocated Selected

Completed Successfully

Process Windows Event Logs Parser for Z6E8KD3N

Completed Successfully

Process Windows Event Logs Parser for JP1572JE36LSNK

Completed Successfully

Process Windows Artifact Parser for Z6E8KD3N

Completed Successfully

Process Windows Artifact Parser for JP1572JE36LSNK

Completed Successfully

Use Magnet AXIOM Process 3.4.1.15164

Add the Z6E8KD3N Logical image into AXIOM Process

Search archives and mobile backups is turned on

Calculate hash values is turned off to speed up processing time.

Uncheck “Find more artifacts” to speed up processing time.

Attempts to locate and parse SQLite Databases

Processing Started

Processing Completed Successfully

```
Summary:
========
Start Time: Sep 17, 2019 08:30:39
End Time: Sep 18, 2019 04:05:18
Search Duration: 19:34:30
Indexing Duration: 00:02:19
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: 1283 items
Carved WebM Video: 55 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: 103169 items
Cloud Services URLs: 71 items
CSV Documents: 12 items
Dating Sites URLs: 55 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: 7 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: 680 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: 30983 items

Google WebP Images: 64 items
Hangul Word Processor: 2 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 PrivacIE 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
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: 24119 items
Passwords and Tokens: 7 items
PDF Documents: 1280 items
Photoshop Files: 76 items
Pictures: 952970 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: 5064 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: 5163 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

Adjust Time Zone to EST (accounting for Daylight Savings.

Build Timeline

Completed Successfully

Build Connections

Could not successfully build connections

Will attempt to build at a later time if necessary

Use Magnet AXIOM Process 3.4.1.15164

Add the JP1572JE36LSNK Logical image into AXIOM Process

Search archives and mobile backups is turned on

Calculate hash values is turned off to speed up processing time.

Uncheck “Find more artifacts” to speed up processing time.

Attempts to locate and parse SQLite Databases

Processing Started

```
Processing Completed Successfully

        Summary:
        ========
        Start Time: Sep 18, 2019 14:01:12
        End Time: Sep 20, 2019 02:31:05
        Search Duration: 36:29:43
        Indexing Duration: 00:01:59
        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): 9669 items
        Carved Audio: 4634 items
        Carved Video: 1361 items
        Carved WebM Video: 38 items
        Classifieds URLs: 84698 items
        Cloud Services URLs: 57 items
        CSV Documents: 18 items
        Dating Sites URLs: 9 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: 7 items
        Excel Documents: 193 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: 809 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: 8882 items
Google Analytics Referral Cookies: 3181 items
Google Analytics Referral Cookies Carved: 7673 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: 20805 items
Google WebP Images: 35 items
Hangul Word Processor: 2 items
Identifiers: 3085 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: 33075 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: 1608 items
Photoshop Files: 99 items
Pictures: 899148 items
Pornography URLs: 3 items
Potential Browser Activity: 45425 items
Potential Facebook Pictures: 3654 items
PowerPoint Documents: 31 items
Prefetch Files - Windows XP/Vista/7: 247 items
QuickBooks Files: 109 items
Rebuilt Webpages: 43866 items
Remote Desktop Protocol: 61 items
RTF Documents: 796 items
Safari History: 4 items
Shellbags: 19087 items
Shipping Site URLs: 1626 items
Social Media URLs: 4100 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: 6035 items
VLC Recently Played Files: 45 items
Web Chat URLs: 5 items
Web Video Fragments: 15 items
WebKit Browser Web History (Carved): 248 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

Completed Successfully

Build Connections

Could not successfully build connections

Will attempt to build at a later time if necessary

SEARCH CRITERIA

User Accounts of Interest

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- Tova NOEL
- Micheal THOMAS
- [redacted]
- [redacted]

Logs, Records, and Count Sheets

8-9-19 through 8-10-19

30 Minute Rounds - Count Logs

8-9-19 at Midnight, 3am, and 5am

8-10-19 at Midnight, 3am, and 5am

10pm to 6am on 8-10-19 computer activity, what was happening

Guards are supposed to walk their section every 30 minutes

Count of every inmate at Midnight, 3am, and 5am

Documents indicating the counts were done (forms) or lack of forms

If they weren't doing their rounds and/or counts, what were they doing?

Who was logged in? - Any user changes?

A solid timeline of any and all activity - Sleeping???

2 to 5 Minutes to do a count, 12am, 3am, 5am

A 30 minute round check takes a minute

6:33 AM Body is found by Thomas

6:45 AM down and transported to hospital

Case Agent Consultation:

Z6E8M349 User Account Logged in at potential time of death is Thomas, Michael

BOP Account: bop19012	SID: S-1-5-21-1823249720-3210992811-1527010081-1102
Logged into System on:	8/10/2019 12:36:56 AM
Logged out of System on:	8/10/2019 5:14:13 AM
Logged into System on:	8/10/2019 6:03:33 AM
Logged out of System on:	8/10/2019 8:55:12 AM

Z6E8K1EV User Account Logged in at potential time of death is Tova Noel

BOP Account: bop61232	SID: S-1-5-21-3548300276-3289552418-2794689317-1126
Logged into System on:	8/9/2019 11:40:28 PM
Logged out of System on:	8/10/2019 10:31:40 AM

BOP uses GroupWise for Email. For instance, we use Microsoft Outlook. This email is not cached, or saved to the computer.

Z6E8M349:	No Cached Email for Michael Thomas
Z6E8K1EV:	No Cached Email for Tova Noel

Case Agent will need to request email from BOP.

Case Agent will need to request BOP files from servers and applications on the BOP network.

Michael Thomas (bop19012) on Z6E8M349

Low Activity for the user during the time frame on Z6E8M349

"SHU 30 CHECK SHEET (CONDENSED)_1.docx" in \Documents\Groupwise

File Created 8/10/19 12:39:31   Last Modified 8/10/19 12:43:33

File is a Check Sheet for each 30 minutes, but is not filled out.

Only File with Time Stamp Information on the day of question.

"~$U 30 CHECK SHEET (CONDENSED)_1.docx" in \Documents\Groupwise

File Created 8/10/19 12:40:28   Last Modified 8/10/19 12:40:28

Tilde is commonly associated as backup files of a file that was opened or is still currently opened.

Possibly indicates the file was saved to the Groupwise location and opened, but never populated.

Network Usage with BOP Applications

http://sallyport.bop.gov/inst/nym/corrsvc/docs/Daily%20Fire%20&%20Security%20Form.pdf

file:///K:/BOPAPPS/Roster/Ver3.1/Roster.accde

file:///I:/GROUPS/SHAREDOC/SHU PAPERWORK, LOCATOR, HARDCOPY/1 - SHU LOCATOR 2019(HARDCOPY).docx

Google Search for "suzuki gsx-r 1000 motorcycle for sale" 8/10/19 01:00:52

Google Search for "suzuki gsx-r 750 motorcycle for sale" on 8/10/19 01:00:52

Bing Search for "cycletrader" on 8/10/19 01:00:24

Bing Search for "espn" on 8/10/19 06:15:03

Internet Usage is consistent with search times

No recorded usage between 01:03:20 and 06:04:30

Edge/Internet Explorer History records File Access within Windows Explorer

file:///C:/Users/bop19012/Desktop/SHU ORDERLY REQUEST 42214.rtf

8/10/2019 00:44:53

Not Located on the Desktop

Potential other files accessed – will continue in depth search

I did locate artifacts indicating that the user profile was used to watch Django Unchained 2012 DVDSCR XVI, but this took place in 5/12/2019 12:00:30 PM

Three Network Shares:

\\NYMC_APPS_SERVER\APPS

\\NYMC_GRPS_SERVER\GRPS

\\NYMC_HOME_SERVER\HOME\HOME\BOP19012

GET THIS!!!!

Tova Noel (bop61232) on Z6E8K1EV

Low Activity for the user during time frame on Z6E8K1EV

No Work Files with Time Stamp Information on the day of question within profile.

Network Usage with BOP Applications

\\NYMC_APPS_SERVER\APPS\BOPAPPS\Roster\Ver3.1\Roster.accde

Google Search for "epp" on 8/10/2019 04:31:33

Google Search for "unum insurance" on 8/10/2019 04:36:00

Google Search for " usajobs" on 8/10/2019 04:39:01

Google Search for "furniture bronx ny" on 8/10/2019 04:48:23

Google Search for "ashleys furniture" on 8/10/2019 04:52:12

Google Search for "KENYATTA TAISTE" on 8/10/2019 05:38:55

Google Search for "latest on epstein in jail" on 8/10/2019 05:42:56 & 8/10/2019 05:52:29

Google Search for "latest on omar amanat" on 8/10/2019 05:53:02

Google Search for "law enforcement discounts" on 8/10/2019 06:17:23

Bing Search for "calendar 2019" on 8/10/2019 4:33:13 AM

Internet Usage: 8/10/19 03:56:00 to 8/10/19 06:19:12

Three Network Shares:

\\NYMC_APPS_SERVER\APPS

\\NYMC_GRPS_SERVER\GRPS

\\NYMC_HOME_SERVER\HOME\HOME\ BOP61232

GET THIS!!!!

Roster.accde: Appears to be a Microsoft Access Database.

Determine what the "Roster" entails – Case Agent

Timeout Information (TimeoutInfo.txt) on 8/14/19 for Magnet AXIOM Processing

```
Data Processor #9 timeout info:
-----------------------------------------------------------
Current search item: Data Processor 9:  Searching [ROOT]\Windows\MEMORY.DMP at offset 54525952
Timestamp: 07/22/2019 06:19:32
Operating System: Microsoft Windows NT 10.0.17134.0
Product Version: 3.2.0.14471
.NET Version: 4.0.30319.42000
Current Locale: en-US
Number Of Processors: 1
  Processor 0 Name: Intel(R) Core(TM) i7-8700K CPU @ 3.70GHz
  Processor 0 64-bit Ready: True
  Processor 0 Cores: 6
  Processor 0 Logical Processors: 12
Memory Available: 63.94 GB
Stack trace:
  at DiscUtils.Compression.Zlibwapi.UncompressX64(IntPtr Dest, Int32& DestLen, IntPtr Source, Int32 SourceLen)
  at DiscUtils.Compression.Zlibwapi.UncompressX64(IntPtr Dest, Int32& DestLen, IntPtr Source, Int32 SourceLen)
  at DiscUtils.Compression.Zlibwapi.Uncompress(Byte[] Dest, Int32 dstOffset, Int32& DestLen, Byte[] Source, Int32 srcOffset,
Int32 SourceLen)
  at DiscUtils.Ewf.EWFStream.ReadChunk(Int32 chunkNo, Byte[] dest, Int32 destOffset)
  at DiscUtils.Ewf.EWFStream.Read(Byte[] buffer, Int32 offset, Int32 count)
  at DiscUtils.ThreadSafeStream.Read(Byte[] buffer, Int32 offset, Int32 count)
  at DiscUtils.SubStream.Read(Byte[] buffer, Int32 offset, Int32 count)
  at DiscUtils.BlockCacheStream.Read(Byte[] buffer, Int32 offset, Int32 count)
  at Magnet.Utilities.Helpers.StreamHelper.ReadFully(Stream stream, Byte[] buffer, Int32 offset, Int32 length)
  at DiscUtils.Ntfs.RawClusterStream.ReadClusters(Int64 startVcn, Int32 count, Byte[] buffer, Int32 offset)
  at DiscUtils.Ntfs.NonResidentDataBuffer.Read(Int64 pos, Byte[] buffer, Int32 offset, Int32 count)
  at DiscUtils.Ntfs.NtfsAttributeBuffer.Read(Int64 pos, Byte[] buffer, Int32 offset, Int32 count)
  at DiscUtils.BufferStream.Read(Byte[] buffer, Int32 offset, Int32 count)
  at DiscUtils.Ntfs.NtfsFileStream.Read(Byte[] buffer, Int32 offset, Int32 count)
  at DiscUtils.SparseStreamLocked.Read(Byte[] buffer, Int32 offset, Int32 count)
  at DiscUtils.ThreadSafeStream.Read(Byte[] buffer, Int32 offset, Int32 count)
  at Magnet.Engine.Features.Searchable.SubStream.ReadInnerStream(Byte[] buffer, Int32 bufferOffset, Int32 readCount, Int64
streamReadPosition)
  at Magnet.Engine.Features.Searchable.SubStream.UpdateCache(Int64 startOffset, Int64 count)
  at Magnet.Engine.Features.Searchable.SubStream.Read(Byte[] buffer, Int32 offset, Int32 count)
  at Magnet.Artifacts.WindowsPrefetchFiles.WindowsPrefetchFileParser.ParseVolumeNameSection(UInt32 headOffset, Int32
sectionNumber)
  at Magnet.Artifacts.WindowsPrefetchFiles.WindowsPrefetchFileParser.ParseSectionD()
  at Magnet.Artifacts.WindowsPrefetchFiles.WindowsPrefetchFileParser.ParseWin7()
  at Magnet.Artifacts.WindowsPrefetchFiles.WindowsPrefetchFileParser.Parse()
  at Magnet.Artifacts.WindowsPrefetchFiles.WindowsXpVista7PrefetchFilesHunter.<Process>d__8.MoveNext()
  at Magnet.Artifacts.Common.Hunters.Hunter.Hunt(IContext context, CancellationToken cancellationToken)
  at Magnet.Engine.Features.ArtifactEngine.<>c__DisplayClass54_2.<HandlePatternMatches>b__1()
  at Magnet.Engine.Features.ArtifactEngine.<>c__DisplayClass57_0`1.<TryWithEnhancedLogging>b__0()
  at Magnet.Utilities.Exceptions.Try.InReleaseMode[T](Func`1 dangerous)
  at Magnet.Engine.Features.ArtifactEngine.HandlePatternMatches(ICarvedHunter hunter, IEnumerable`1 matches)
  at Magnet.Engine.Features.ArtifactEngine.<>c__DisplayClass53_0.<HandlePatternMatchesGenerator>b__0(IEnumerable`1
matches, CancellationToken token)
  at Magnet.Matching.SinglePass.ByteScanner`1.RunDeferredCallbacks()
  at Magnet.Matching.SinglePass.PfacNative.PfacNativeByteScanner`1.Scan(Int32 startIdx, Int32 maxNumBytes)
  at Magnet.Engine.Features.ArtifactEngine.<>c__DisplayClass58_0.<TryWithEnhancedLogging>b__0()
  at Magnet.Utilities.Exceptions.Try.InReleaseMode(Action dangerous)
  at Magnet.Engine.Features.ArtifactEngine.SinglePassByteCarve(IEngineSearchable searchable, Int32 startOffset,
IWorkerInformation workerInformation)
```

```
  at Magnet.Engine.Features.ArtifactEngine.Carve(IEngineSearchable searchable, IReadOnlyCollection`1 huntStatuses, Int32
startOffset, IWorkerInformation workerInformation, IPerformanceMetrics performanceMetrics, ManualResetEvent
pauseTrigger)
  at Magnet.Engine.Common.Multithreading.CarvedWorkItem.DoWork(IArtifactEngine artifactEngine, IWorkerInformation
workerInformation, IPlatformTranslator platformTranslator, ManualResetEvent pauseTrigger)
  at Magnet.Engine.Common.Multithreading.WorkerThread.ProcessWorkItem(IWorkItem workItem, ICaseWriter caseWriter,
IArtifactEngine engine)
  at Magnet.Engine.Common.Multithreading.WorkerThread.DoWork()
  at System.Threading.ExecutionContext.RunInternal(ExecutionContext executionContext, ContextCallback callback, Object
state, Boolean preserveSyncCtx)
  at System.Threading.ExecutionContext.Run(ExecutionContext executionContext, ContextCallback callback, Object state,
Boolean preserveSyncCtx)
  at System.Threading.ExecutionContext.Run(ExecutionContext executionContext, ContextCallback callback, Object state)
  at System.Threading.ThreadHelper.ThreadStart()

Work Log:
Starting carving using LimeFrostSearchCarvedHunter
Hunter LimeFrostSearchCarvedHunter took 00:00:00.00 to carve
Starting carving using YahooMessengerHunter
Hunter YahooMessengerHunter took 00:00:00.00 to carve
Starting carving using Skype4xCarvedHunter
Hunter Skype4xCarvedHunter took 00:00:00.00 to carve
Starting carving using AvcSequenceHunter
Hunter AvcSequenceHunter took 00:00:00.00 to carve
Starting carving using Skype5x6xCarvedHunter
Hunter Skype5x6xCarvedHunter took 00:00:00.00 to carve
Starting carving using CarvedPictureHunter
Hunter CarvedPictureHunter took 00:00:00.03 to carve
Starting carving using WindowsXpVista7PrefetchFilesHunter

Data Processor #8 timeout info:
-----------------------------------------------------------
Current search item: Data Processor 8:  Searching [ROOT]\Windows\MEMORY.DMP at offset 54525952
Timestamp: 07/23/2019 12:52:25
Operating System: Microsoft Windows NT 10.0.17134.0
Product Version: 3.2.0.14471
.NET Version: 4.0.30319.42000
Current Locale: en-US
Number Of Processors: 1
  Processor 0 Name: Intel(R) Core(TM) i7-8700K CPU @ 3.70GHz
  Processor 0 64-bit Ready: True
  Processor 0 Cores: 6
  Processor 0 Logical Processors: 12
Memory Available: 63.94 GB
Stack trace:
  at DiscUtils.Compression.Zlibwapi.UncompressX64(IntPtr Dest, Int32& DestLen, IntPtr Source, Int32 SourceLen)
  at DiscUtils.Compression.Zlibwapi.UncompressX64(IntPtr Dest, Int32& DestLen, IntPtr Source, Int32 SourceLen)
  at DiscUtils.Compression.Zlibwapi.Uncompress(Byte[] Dest, Int32 dstOffset, Int32& DestLen, Byte[] Source, Int32 srcOffset,
Int32 SourceLen)
  at DiscUtils.Ewf.EWFStream.ReadChunk(Int32 chunkNo, Byte[] dest, Int32 destOffset)
  at DiscUtils.Ewf.EWFStream.Read(Byte[] buffer, Int32 offset, Int32 count)
  at DiscUtils.ThreadSafeStream.Read(Byte[] buffer, Int32 offset, Int32 count)
  at DiscUtils.SubStream.Read(Byte[] buffer, Int32 offset, Int32 count)
  at DiscUtils.BlockCacheStream.Read(Byte[] buffer, Int32 offset, Int32 count)
  at Magnet.Utilities.Helpers.StreamHelper.ReadFully(Stream stream, Byte[] buffer, Int32 offset, Int32 length)
  at DiscUtils.Ntfs.RawClusterStream.ReadClusters(Int64 startVcn, Int32 count, Byte[] buffer, Int32 offset)
  at DiscUtils.Ntfs.NonResidentDataBuffer.Read(Int64 pos, Byte[] buffer, Int32 offset, Int32 count)
  at DiscUtils.Ntfs.NtfsAttributeBuffer.Read(Int64 pos, Byte[] buffer, Int32 offset, Int32 count)
```

```
   at DiscUtils.BufferStream.Read(Byte[] buffer, Int32 offset, Int32 count)
   at DiscUtils.Ntfs.NtfsFileStream.Read(Byte[] buffer, Int32 offset, Int32 count)
   at DiscUtils.SparseStreamLocked.Read(Byte[] buffer, Int32 offset, Int32 count)
   at DiscUtils.ThreadSafeStream.Read(Byte[] buffer, Int32 offset, Int32 count)
   at Magnet.Engine.Features.Searchable.SubStream.ReadInnerStream(Byte[] buffer, Int32 bufferOffset, Int32 readCount, Int64
streamReadPosition)
   at Magnet.Engine.Features.Searchable.SubStream.UpdateCache(Int64 startOffset, Int64 count)
   at Magnet.Engine.Features.Searchable.SubStream.Read(Byte[] buffer, Int32 offset, Int32 count)
   at Magnet.Artifacts.WindowsPrefetchFiles.WindowsPrefetchFileParser.ParseVolumeNameSection(UInt32 headOffset, Int32
sectionNumber)
   at Magnet.Artifacts.WindowsPrefetchFiles.WindowsPrefetchFileParser.ParseSectionD()
   at Magnet.Artifacts.WindowsPrefetchFiles.WindowsPrefetchFileParser.ParseWin7()
   at Magnet.Artifacts.WindowsPrefetchFiles.WindowsPrefetchFileParser.Parse()
   at Magnet.Artifacts.WindowsPrefetchFiles.WindowsXpVista7PrefetchFilesHunter.<Process>d__8.MoveNext()
   at Magnet.Artifacts.Common.Hunters.Hunter.Hunt(IContext context, CancellationToken cancellationToken)
   at Magnet.Engine.Features.ArtifactEngine.<>c__DisplayClass54_2.<HandlePatternMatches>b__1()
   at Magnet.Engine.Features.ArtifactEngine.<>c__DisplayClass57_0`1.<TryWithEnhancedLogging>b__0()
   at Magnet.Utilities.Exceptions.Try.InReleaseMode[T](Func`1 dangerous)
   at Magnet.Engine.Features.ArtifactEngine.HandlePatternMatches(ICarvedHunter hunter, IEnumerable`1 matches)
   at Magnet.Engine.Features.ArtifactEngine.<>c__DisplayClass53_0.<HandlePatternMatchesGenerator>b__0(IEnumerable`1
matches, CancellationToken token)
   at Magnet.Matching.SinglePass.ByteScanner`1.RunDeferredCallbacks()
   at Magnet.Matching.SinglePass.PfacNative.PfacNativeByteScanner`1.Scan(Int32 startIdx, Int32 maxNumBytes)
   at Magnet.Engine.Features.ArtifactEngine.<>c__DisplayClass58_0.<TryWithEnhancedLogging>b__0()
   at Magnet.Utilities.Exceptions.Try.InReleaseMode(Action dangerous)
   at Magnet.Engine.Features.ArtifactEngine.SinglePassByteCarve(IEngineSearchable searchable, Int32 startOffset,
IWorkerInformation workerInformation)
   at Magnet.Engine.Features.ArtifactEngine.Carve(IEngineSearchable searchable, IReadOnlyCollection`1 huntStatuses, Int32
startOffset, IWorkerInformation workerInformation, IPerformanceMetrics performanceMetrics, ManualResetEvent
pauseTrigger)
   at Magnet.Engine.Common.Multithreading.CarvedWorkItem.DoWork(IArtifactEngine artifactEngine, IWorkerInformation
workerInformation, IPlatformTranslator platformTranslator, ManualResetEvent pauseTrigger)
   at Magnet.Engine.Common.Multithreading.WorkerThread.ProcessWorkItem(IWorkItem workItem, ICaseWriter caseWriter,
IArtifactEngine engine)
   at Magnet.Engine.Common.Multithreading.WorkerThread.DoWork()
   at System.Threading.ExecutionContext.RunInternal(ExecutionContext executionContext, ContextCallback callback, Object
state, Boolean preserveSyncCtx)
   at System.Threading.ExecutionContext.Run(ExecutionContext executionContext, ContextCallback callback, Object state,
Boolean preserveSyncCtx)
   at System.Threading.ExecutionContext.Run(ExecutionContext executionContext, ContextCallback callback, Object state)
   at System.Threading.ThreadHelper.ThreadStart()

Work Log:
Starting carving using LimeFrostSearchCarvedHunter
Hunter LimeFrostSearchCarvedHunter took 00:00:00.01 to carve
Starting carving using YahooMessengerHunter
Hunter YahooMessengerHunter took 00:00:00.00 to carve
Starting carving using Skype4xCarvedHunter
Hunter Skype4xCarvedHunter took 00:00:00.00 to carve
Starting carving using AvcSequenceHunter
Hunter AvcSequenceHunter took 00:00:00.00 to carve
Starting carving using Skype5x6xCarvedHunter
Hunter Skype5x6xCarvedHunter took 00:00:00.00 to carve
Starting carving using CarvedPictureHunter
Hunter CarvedPictureHunter took 00:00:00.03 to carve
Starting carving using WindowsXpVista7PrefetchFilesHunter

Data Processor #3 timeout info:
```

```
------------------------------------------------------------
Current search item: Data Processor 3:  Parsing
[ROOT]\Windows.old\WINDOWS\SoftwareDistribution\Download\e6ed64fcea4f307d9e44948f04d21901\AMD64_Microsoft.M
odernApps.Client.professional~~AMD64~~0.0.0.0\microsoft.skypeapp_kzf8qxf38zg5c\microsoft.skypeapp_11.18.596.0_x64__k
zf8qxf38zg5c\skypeapp\designs\emoticons\large\poolparty.png
Timestamp: 07/31/2019 03:53:29
Operating System: Microsoft Windows NT 10.0.17134.0
Product Version: 3.2.0.14471
.NET Version: 4.0.30319.42000
Current Locale: en-US
Number Of Processors: 1
  Processor 0 Name: Intel(R) Core(TM) i7-8700K CPU @ 3.70GHz
  Processor 0 64-bit Ready: True
  Processor 0 Cores: 6
  Processor 0 Logical Processors: 12
Memory Available: 63.94 GB
Stack trace:
  at System.Threading.Monitor.Enter(Object obj)
  at DiscUtils.SparseStreamLocked.set_Position(Int64 value)
  at Magnet.Engine.Features.Searchable.SubStream.Reset()
  at Magnet.Engine.Features.ArtifactEngine.NonCarve(IEngineSearchable searchable, IWorkerInformation workerInformation,
IPerformanceMetrics performanceMetrics, ManualResetEvent pauseTrigger)
  at Magnet.Engine.Common.Multithreading.NonCarvedWorkItem.Parse(SearchInformation searchInfo, IArtifactEngine
artifactEngine, IWorkerInformation workerInformation, IPlatformTranslator platformTranslator, ManualResetEvent
pauseTrigger)
  at Magnet.Engine.Common.Multithreading.NonCarvedWorkItem.DoWork(IArtifactEngine artifactEngine, IWorkerInformation
workerInformation, IPlatformTranslator platformTranslator, ManualResetEvent pauseTrigger)
  at Magnet.Engine.Common.Multithreading.WorkerThread.ProcessWorkItem(IWorkItem workItem, ICaseWriter caseWriter,
IArtifactEngine engine)
  at Magnet.Engine.Common.Multithreading.WorkerThread.DoWork()
  at System.Threading.ExecutionContext.RunInternal(ExecutionContext executionContext, ContextCallback callback, Object
state, Boolean preserveSyncCtx)
  at System.Threading.ExecutionContext.Run(ExecutionContext executionContext, ContextCallback callback, Object state,
Boolean preserveSyncCtx)
  at System.Threading.ExecutionContext.Run(ExecutionContext executionContext, ContextCallback callback, Object state)
  at System.Threading.ThreadHelper.ThreadStart()

Work Log:
Starting noncarving using StandardPictureHunter

Data Processor #4 timeout info:
------------------------------------------------------------
Current search item: Data Processor 4:  Searching [ROOT]\Windows\MEMORY.DMP at offset 130023424
Timestamp: 08/14/2019 10:17:25
Operating System: Microsoft Windows NT 10.0.17134.0
Product Version: 3.4.1.15164
.NET Version: 4.0.30319.42000
Current Locale: en-US
Number Of Processors: 1
  Processor 0 Name: Intel(R) Core(TM) i7-8700K CPU @ 3.70GHz
  Processor 0 64-bit Ready: True
  Processor 0 Cores: 6
  Processor 0 Logical Processors: 12
Memory Available: 63.94 GB
Stack trace:
  at Microsoft.Win32.Win32Native.CloseHandle(IntPtr handle)
  at Microsoft.Win32.Win32Native.CloseHandle(IntPtr handle)
  at System.Runtime.InteropServices.SafeHandle.InternalDispose()
```

```
   at System.IO.FileStream.Dispose(Boolean disposing)
   at System.IO.Stream.Close()
   at log4net.Appender.FileAppender.LockingModelBase.CloseStream(Stream stream)
   at log4net.Appender.FileAppender.MinimalLock.ReleaseLock()
   at log4net.Appender.FileAppender.LockingStream.ReleaseLock()
   at log4net.Appender.FileAppender.Append(LoggingEvent loggingEvent)
   at log4net.Appender.AppenderSkeleton.DoAppend(LoggingEvent loggingEvent)
   at log4net.Util.AppenderAttachedImpl.AppendLoopOnAppenders(LoggingEvent loggingEvent)
   at log4net.Repository.Hierarchy.Logger.CallAppenders(LoggingEvent loggingEvent)
   at log4net.Repository.Hierarchy.Logger.Log(Type callerStackBoundaryDeclaringType, Level level, Object message, Exception
exception)
   at log4net.Core.LogImpl.Debug(Object message)
   at Magnet.Artifacts.WindowsPrefetchFiles.WindowsPrefetchFileParser.Log(String message, Exception e)
   at Magnet.Artifacts.WindowsPrefetchFiles.WindowsPrefetchFileParser.ParseVolumeNameSection(UInt32 headOffset, Int32
sectionNumber)
   at Magnet.Artifacts.WindowsPrefetchFiles.WindowsPrefetchFileParser.ParseSectionD()
   at Magnet.Artifacts.WindowsPrefetchFiles.WindowsPrefetchFileParser.ParseWin7()
   at Magnet.Artifacts.WindowsPrefetchFiles.WindowsPrefetchFileParser.Parse()
   at Magnet.Artifacts.WindowsPrefetchFiles.WindowsXpVista7PrefetchFilesHunter.<Process>d__8.MoveNext()
   at Magnet.Artifacts.Common.Hunters.Hunter.Hunt(IContext context, CancellationToken cancellationToken)
   at Magnet.Engine.Features.ArtifactEngine.<>c__DisplayClass54_2.<HandlePatternMatches>b__1()
   at Magnet.Engine.Features.ArtifactEngine.<>c__DisplayClass57_0`1.<TryWithEnhancedLogging>b__0()
   at Magnet.Utilities.Exceptions.Try.InReleaseMode[T](Func`1 dangerous)
   at Magnet.Engine.Features.ArtifactEngine.HandlePatternMatches(ICarvedHunter hunter, IEnumerable`1 matches)
   at Magnet.Engine.Features.ArtifactEngine.<>c__DisplayClass53_0.<HandlePatternMatchesGenerator>b__0(IEnumerable`1
matches, CancellationToken token)
   at Magnet.Matching.SinglePass.ByteScanner`1.RunDeferredCallbacks()
   at Magnet.Matching.SinglePass.PfacNative.PfacNativeByteScanner`1.Scan(Int32 startIdx, Int32 maxNumBytes)
   at Magnet.Engine.Features.ArtifactEngine.<>c__DisplayClass58_0.<TryWithEnhancedLogging>b__0()
   at Magnet.Utilities.Exceptions.Try.InReleaseMode(Action dangerous)
   at Magnet.Engine.Features.ArtifactEngine.SinglePassByteCarve(IEngineSearchable searchable, Int32 startOffset,
IWorkerInformation workerInformation)
   at Magnet.Engine.Features.ArtifactEngine.Carve(IEngineSearchable searchable, IReadOnlyCollection`1 huntStatuses, Int32
startOffset, IWorkerInformation workerInformation, IPerformanceMetrics performanceMetrics, ManualResetEvent
pauseTrigger)
   at Magnet.Engine.Common.Multithreading.CarvedWorkItem.DoWork(IArtifactEngine artifactEngine, IWorkerInformation
workerInformation, IPlatformTranslator platformTranslator, ManualResetEvent pauseTrigger)
   at Magnet.Engine.Common.Multithreading.WorkerThread.ProcessWorkItem(IWorkItem workItem, ICaseWriter caseWriter,
IArtifactEngine engine)
   at Magnet.Engine.Common.Multithreading.WorkerThread.DoWork()
   at System.Threading.ExecutionContext.RunInternal(ExecutionContext executionContext, ContextCallback callback, Object
state, Boolean preserveSyncCtx)
   at System.Threading.ExecutionContext.Run(ExecutionContext executionContext, ContextCallback callback, Object state,
Boolean preserveSyncCtx)
   at System.Threading.ExecutionContext.Run(ExecutionContext executionContext, ContextCallback callback, Object state)
   at System.Threading.ThreadHelper.ThreadStart()

Work Log:
Starting carving using LimeFrostSearchCarvedHunter
Hunter LimeFrostSearchCarvedHunter took 00:00:00.00 to carve
Starting carving using Skype4xCarvedHunter
Hunter Skype4xCarvedHunter took 00:00:00.01 to carve
Starting carving using Skype5x6xCarvedHunter
Hunter Skype5x6xCarvedHunter took 00:00:00.00 to carve
Starting carving using CarvedPictureHunter
Hunter CarvedPictureHunter took 00:00:00.00 to carve
Starting carving using YahooMessengerHunter
Hunter YahooMessengerHunter took 00:00:00.00 to carve
```

```
Starting carving using SpeexAudioPacketHunter
Hunter SpeexAudioPacketHunter took 00:00:00.00 to carve
Starting carving using AvcSequenceHunter
Hunter AvcSequenceHunter took 00:00:00.00 to carve
Starting carving using Vp6Hunter
Hunter Vp6Hunter took 00:00:00.00 to carve
Starting carving using SearchKeywordsHunter
Hunter SearchKeywordsHunter took 00:00:00.00 to carve
Starting carving using CarvedVideosHunter
Hunter CarvedVideosHunter took 00:00:00.00 to carve
Starting carving using CompoundFileCarvingHunter
Hunter CompoundFileCarvingHunter took 00:00:00.00 to carve
Starting carving using CompoundFileCarvingHunter
Hunter CompoundFileCarvingHunter took 00:00:00.00 to carve
Starting carving using CompoundFileCarvingHunter
Hunter CompoundFileCarvingHunter took 00:00:00.00 to carve
Starting carving using WindowsXpVista7PrefetchFilesHunter
```

Timeout Information (TimeoutInfo.txt) on 8/15/19 for Magnet AXIOM Processing

```
Data Processor #5 timeout info:
-----------------------------------------------------------
Current search item: Data Processor 5:  Searching [ROOT]\Windows\MEMORY.DMP at offset 130023424
Timestamp: 08/15/2019 11:16:33
Operating System: Microsoft Windows NT 10.0.17134.0
Product Version: 3.4.1.15164
.NET Version: 4.0.30319.42000
Current Locale: en-US
Number Of Processors: 1
  Processor 0 Name: Intel(R) Core(TM) i7-8700K CPU @ 3.70GHz
  Processor 0 64-bit Ready: True
  Processor 0 Cores: 6
  Processor 0 Logical Processors: 12
Memory Available: 63.94 GB
Stack trace:
  at Microsoft.Win32.Win32Native.CloseHandle(IntPtr handle)
  at Microsoft.Win32.Win32Native.CloseHandle(IntPtr handle)
  at System.Runtime.InteropServices.SafeHandle.InternalDispose()
  at System.IO.FileStream.Dispose(Boolean disposing)
  at System.IO.Stream.Close()
  at log4net.Appender.FileAppender.LockingModelBase.CloseStream(Stream stream)
  at log4net.Appender.FileAppender.MinimalLock.ReleaseLock()
  at log4net.Appender.FileAppender.LockingStream.ReleaseLock()
  at log4net.Appender.FileAppender.Append(LoggingEvent loggingEvent)
  at log4net.Appender.AppenderSkeleton.DoAppend(LoggingEvent loggingEvent)
  at log4net.Util.AppenderAttachedImpl.AppendLoopOnAppenders(LoggingEvent loggingEvent)
  at log4net.Repository.Hierarchy.Logger.CallAppenders(LoggingEvent loggingEvent)
  at log4net.Repository.Hierarchy.Logger.Log(Type callerStackBoundaryDeclaringType, Level level, Object message,
Exception exception)
  at log4net.Core.LogImpl.Debug(Object message)
  at Magnet.Artifacts.WindowsPrefetchFiles.WindowsPrefetchFileParser.Log(String message, Exception e)
  at Magnet.Artifacts.WindowsPrefetchFiles.WindowsPrefetchFileParser.ParseVolumeNameSection(UInt32
headOffset, Int32 sectionNumber)
  at Magnet.Artifacts.WindowsPrefetchFiles.WindowsPrefetchFileParser.ParseSectionD()
  at Magnet.Artifacts.WindowsPrefetchFiles.WindowsPrefetchFileParser.ParseWin7()
  at Magnet.Artifacts.WindowsPrefetchFiles.WindowsPrefetchFileParser.Parse()
  at Magnet.Artifacts.WindowsPrefetchFiles.WindowsXpVista7PrefetchFilesHunter.<Process>d__8.MoveNext()
  at Magnet.Artifacts.Common.Hunters.Hunter.Hunt(IContext context, CancellationToken cancellationToken)
  at Magnet.Engine.Features.ArtifactEngine.<>c__DisplayClass54_2.<HandlePatternMatches>b__1()
  at Magnet.Engine.Features.ArtifactEngine.<>c__DisplayClass57_0`1.<TryWithEnhancedLogging>b__0()
  at Magnet.Utilities.Exceptions.Try.InReleaseMode[T](Func`1 dangerous)
  at Magnet.Engine.Features.ArtifactEngine.HandlePatternMatches(ICarvedHunter hunter, IEnumerable`1
matches)
  at
Magnet.Engine.Features.ArtifactEngine.<>c__DisplayClass53_0.<HandlePatternMatchesGenerator>b__0(IEnumera
ble`1 matches, CancellationToken token)
  at Magnet.Matching.SinglePass.ByteScanner`1.RunDeferredCallbacks()
  at Magnet.Matching.SinglePass.PfacNative.PfacNativeByteScanner`1.Scan(Int32 startIdx, Int32 maxNumBytes)
  at Magnet.Engine.Features.ArtifactEngine.<>c__DisplayClass58_0.<TryWithEnhancedLogging>b__0()
  at Magnet.Utilities.Exceptions.Try.InReleaseMode(Action dangerous)
```

```
   at Magnet.Engine.Features.ArtifactEngine.SinglePassByteCarve(IEngineSearchable searchable, Int32 startOffset,
IWorkerInformation workerInformation)
   at Magnet.Engine.Features.ArtifactEngine.Carve(IEngineSearchable searchable, IReadOnlyCollection`1
huntStatuses, Int32 startOffset, IWorkerInformation workerInformation, IPerformanceMetrics
performanceMetrics, ManualResetEvent pauseTrigger)
   at Magnet.Engine.Common.Multithreading.CarvedWorkItem.DoWork(IArtifactEngine artifactEngine,
IWorkerInformation workerInformation, IPlatformTranslator platformTranslator, ManualResetEvent pauseTrigger)
   at Magnet.Engine.Common.Multithreading.WorkerThread.ProcessWorkItem(IWorkItem workItem, ICaseWriter
caseWriter, IArtifactEngine engine)
   at Magnet.Engine.Common.Multithreading.WorkerThread.DoWork()
   at System.Threading.ExecutionContext.RunInternal(ExecutionContext executionContext, ContextCallback
callback, Object state, Boolean preserveSyncCtx)
   at System.Threading.ExecutionContext.Run(ExecutionContext executionContext, ContextCallback callback, Object
state, Boolean preserveSyncCtx)
   at System.Threading.ExecutionContext.Run(ExecutionContext executionContext, ContextCallback callback, Object
state)
   at System.Threading.ThreadHelper.ThreadStart()

Work Log:
Starting carving using LimeFrostSearchCarvedHunter
Hunter LimeFrostSearchCarvedHunter took 00:00:00.00 to carve
Starting carving using Skype4xCarvedHunter
Hunter Skype4xCarvedHunter took 00:00:00.00 to carve
Starting carving using Skype5x6xCarvedHunter
Hunter Skype5x6xCarvedHunter took 00:00:00.00 to carve
Starting carving using CarvedPictureHunter
Hunter CarvedPictureHunter took 00:00:00.00 to carve
Starting carving using YahooMessengerHunter
Hunter YahooMessengerHunter took 00:00:00.00 to carve
Starting carving using SpeexAudioPacketHunter
Hunter SpeexAudioPacketHunter took 00:00:00.00 to carve
Starting carving using AvcSequenceHunter
Hunter AvcSequenceHunter took 00:00:00.00 to carve
Starting carving using Vp6Hunter
Hunter Vp6Hunter took 00:00:00.00 to carve
Starting carving using SearchKeywordsHunter
Hunter SearchKeywordsHunter took 00:00:00.00 to carve
Starting carving using CarvedVideosHunter
Hunter CarvedVideosHunter took 00:00:00.00 to carve
Starting carving using CompoundFileCarvingHunter
Hunter CompoundFileCarvingHunter took 00:00:00.00 to carve
Starting carving using CompoundFileCarvingHunter
Hunter CompoundFileCarvingHunter took 00:00:00.00 to carve
Starting carving using CompoundFileCarvingHunter
Hunter CompoundFileCarvingHunter took 00:00:00.00 to carve
Starting carving using WindowsXpVista7PrefetchFilesHunter
```

Timeout Information (TimeoutInfo.txt) on 8/15/19 for Magnet AXIOM Processing

```
Data Processor #8 timeout info:
------------------------------------------------------------
Current search item: Data Processor 8:  Searching [ROOT]\Program Files\Windows Mail\MSOERES.dll at offset 0
Timestamp: 08/16/2019 09:12:09
Operating System: Microsoft Windows NT 10.0.17134.0
Product Version: 3.4.1.15164
.NET Version: 4.0.30319.42000
Current Locale: en-US
Number Of Processors: 1
  Processor 0 Name: Intel(R) Core(TM) i7-8700K CPU @ 3.70GHz
  Processor 0 64-bit Ready: True
  Processor 0 Cores: 6
  Processor 0 Logical Processors: 12
Memory Available: 63.94 GB
Stack trace:
  at FFmpegLibrary.FFmpegInvoke.av_register_all()
  at FFmpegLibrary.FFmpegInvoke.av_register_all()
  at FFmpegLibrary.FFmpegAPI..ctor()
  at Magnet.Engine.Features.Features.FFmpegFeature.GetMetadata(String filename)
  at Magnet.Engine.Features.Features.VideoFeature.GetMetadata(String filePath)
  at Magnet.Engine.Features.Features.VideoFeature.GetVideoLengthAndRotation(String filename, Nullable`1&
length, Int32& rotation)
  at Magnet.Engine.Features.Features.VideoFeature.GetThumbnail(String filename, Boolean getSkintone,
Nullable`1& averageSkinPercentage)
  at Magnet.Artifacts.Common.Utilities.Helpers.VideoHelpers.GetThumbnailAndSkinTone(String filename, Byte[]&
thumbnailBytes, Nullable`1& averageSkinPercentage)
  at Magnet.Artifacts.Video.CarvedVideosHunter.CreateHit(ISearchable searchable, String format, String
contentType, Int64 fileSize, Func`2 vidDataFunc, Int64 foundSpot)
  at Magnet.Artifacts.Video.CarvedVideosHunter.ParseAVIFile(ISearchable searchable, Int64 foundSpot)
  at Magnet.Artifacts.Video.CarvedVideosHunter.<Process>d__30.MoveNext()
  at Magnet.Artifacts.Common.Hunters.Hunter.Hunt(IContext context, CancellationToken cancellationToken)
  at Magnet.Engine.Features.ArtifactEngine.<>c__DisplayClass54_2.<HandlePatternMatches>b__1()
  at Magnet.Engine.Features.ArtifactEngine.<>c__DisplayClass57_0`1.<TryWithEnhancedLogging>b__0()
  at Magnet.Utilities.Exceptions.Try.InReleaseMode[T](Func`1 dangerous)
  at Magnet.Engine.Features.ArtifactEngine.HandlePatternMatches(ICarvedHunter hunter, IEnumerable`1
matches)
  at
Magnet.Engine.Features.ArtifactEngine.<>c__DisplayClass53_0.<HandlePatternMatchesGenerator>b__0(IEnumera
ble`1 matches, CancellationToken token)
  at Magnet.Matching.SinglePass.ByteScanner`1.RunDeferredCallbacks()
  at Magnet.Matching.SinglePass.PfacNative.PfacNativeByteScanner`1.Scan(Int32 startIdx, Int32 maxNumBytes)
  at Magnet.Engine.Features.ArtifactEngine.<>c__DisplayClass58_0.<TryWithEnhancedLogging>b__0()
  at Magnet.Utilities.Exceptions.Try.InReleaseMode(Action dangerous)
  at Magnet.Engine.Features.ArtifactEngine.SinglePassByteCarve(IEngineSearchable searchable, Int32 startOffset,
IWorkerInformation workerInformation)
  at Magnet.Engine.Features.ArtifactEngine.Carve(IEngineSearchable searchable, IReadOnlyCollection`1
huntStatuses, Int32 startOffset, IWorkerInformation workerInformation, IPerformanceMetrics
performanceMetrics, ManualResetEvent pauseTrigger)
  at Magnet.Engine.Common.Multithreading.CarvedWorkItem.DoWork(IArtifactEngine artifactEngine,
IWorkerInformation workerInformation, IPlatformTranslator platformTranslator, ManualResetEvent pauseTrigger)
```

```
  at Magnet.Engine.Common.Multithreading.WorkerThread.ProcessWorkItem(IWorkItem workItem, ICaseWriter caseWriter, IArtifactEngine engine)
  at Magnet.Engine.Common.Multithreading.WorkerThread.DoWork()
  at System.Threading.ExecutionContext.RunInternal(ExecutionContext executionContext, ContextCallback callback, Object state, Boolean preserveSyncCtx)
  at System.Threading.ExecutionContext.Run(ExecutionContext executionContext, ContextCallback callback, Object state, Boolean preserveSyncCtx)
  at System.Threading.ExecutionContext.Run(ExecutionContext executionContext, ContextCallback callback, Object state)
  at System.Threading.ThreadHelper.ThreadStart()

Work Log:
Starting carving using YahooMessengerHunter
Hunter YahooMessengerHunter took 00:00:00.00 to carve
Starting carving using CarvedPictureHunter
Hunter CarvedPictureHunter took 00:00:00.09 to carve
Starting carving using IePrivateHunter
Hunter IePrivateHunter took 00:00:00.00 to carve
Starting carving using Skype4xCarvedHunter
Hunter Skype4xCarvedHunter took 00:00:00.00 to carve
Starting carving using Vp6Hunter
Hunter Vp6Hunter took 00:00:00.00 to carve
Starting carving using LimeFrostSearchCarvedHunter
Hunter LimeFrostSearchCarvedHunter took 00:00:00.00 to carve
Starting carving using SpeexAudioPacketHunter
Hunter SpeexAudioPacketHunter took 00:00:00.00 to carve
Starting carving using AvcSequenceHunter
Hunter AvcSequenceHunter took 00:00:00.00 to carve
Starting carving using CarvedVideosHunter

Data Processor #7 timeout info:
------------------------------------------------------------
Current search item: Data Processor 7:  Searching [ROOT]\Program Files\Windows Defender\MsMpRes.dll at offset 0
Timestamp: 08/16/2019 09:12:20
Operating System: Microsoft Windows NT 10.0.17134.0
Product Version: 3.4.1.15164
.NET Version: 4.0.30319.42000
Current Locale: en-US
Number Of Processors: 1
  Processor 0 Name: Intel(R) Core(TM) i7-8700K CPU @ 3.70GHz
  Processor 0 64-bit Ready: True
  Processor 0 Cores: 6
  Processor 0 Logical Processors: 12
Memory Available: 63.94 GB
Stack trace:
  at FFmpegLibrary.FFmpegInvoke.av_register_all()
  at FFmpegLibrary.FFmpegInvoke.av_register_all()
  at FFmpegLibrary.FFmpegAPI..ctor()
  at Magnet.Engine.Features.Features.FFmpegFeature.GetMetadata(String filename)
  at Magnet.Engine.Features.Features.VideoFeature.GetMetadata(String filePath)
  at Magnet.Engine.Features.Features.VideoFeature.GetVideoLengthAndRotation(String filename, Nullable`1& length, Int32& rotation)
  at Magnet.Engine.Features.Features.VideoFeature.GetThumbnail(String filename, Boolean getSkintone,
Nullable`1& averageSkinPercentage)
  at Magnet.Artifacts.Common.Utilities.Helpers.VideoHelpers.GetThumbnailAndSkinTone(String filename, Byte[]&
thumbnailBytes, Nullable`1& averageSkinPercentage)
  at Magnet.Artifacts.Video.CarvedVideosHunter.CreateHit(ISearchable searchable, String format, String
contentType, Int64 fileSize, Func`2 vidDataFunc, Int64 foundSpot)
  at Magnet.Artifacts.Video.CarvedVideosHunter.ParseAVIFile(ISearchable searchable, Int64 foundSpot)
  at Magnet.Artifacts.Video.CarvedVideosHunter.<Process>d__30.MoveNext()
  at Magnet.Artifacts.Common.Hunters.Hunter.Hunt(IContext context, CancellationToken cancellationToken)
  at Magnet.Engine.Features.ArtifactEngine.<>c__DisplayClass54_2.<HandlePatternMatches>b__1()
  at Magnet.Engine.Features.ArtifactEngine.<>c__DisplayClass57_0`1.<TryWithEnhancedLogging>b__0()
  at Magnet.Utilities.Exceptions.Try.InReleaseMode[T](Func`1 dangerous)
  at Magnet.Engine.Features.ArtifactEngine.HandlePatternMatches(ICarvedHunter hunter, IEnumerable`1
matches)
  at
Magnet.Engine.Features.ArtifactEngine.<>c__DisplayClass53_0.<HandlePatternMatchesGenerator>b__0(IEnumera
ble`1 matches, CancellationToken token)
  at Magnet.Matching.SinglePass.ByteScanner`1.RunDeferredCallbacks()
  at Magnet.Matching.SinglePass.PfacNative.PfacNativeByteScanner`1.Scan(Int32 startIdx, Int32 maxNumBytes)
  at Magnet.Engine.Features.ArtifactEngine.<>c__DisplayClass58_0.<TryWithEnhancedLogging>b__0()
  at Magnet.Utilities.Exceptions.Try.InReleaseMode(Action dangerous)
  at Magnet.Engine.Features.ArtifactEngine.SinglePassByteCarve(IEngineSearchable searchable, Int32 startOffset,
IWorkerInformation workerInformation)
  at Magnet.Engine.Features.ArtifactEngine.Carve(IEngineSearchable searchable, IReadOnlyCollection`1
huntStatuses, Int32 startOffset, IWorkerInformation workerInformation, IPerformanceMetrics
performanceMetrics, ManualResetEvent pauseTrigger)
  at Magnet.Engine.Common.Multithreading.CarvedWorkItem.DoWork(IArtifactEngine artifactEngine,
IWorkerInformation workerInformation, IPlatformTranslator platformTranslator, ManualResetEvent pauseTrigger)
  at Magnet.Engine.Common.Multithreading.WorkerThread.ProcessWorkItem(IWorkItem workItem, ICaseWriter
caseWriter, IArtifactEngine engine)
  at Magnet.Engine.Common.Multithreading.WorkerThread.DoWork()
  at System.Threading.ExecutionContext.RunInternal(ExecutionContext executionContext, ContextCallback
callback, Object state, Boolean preserveSyncCtx)
  at System.Threading.ExecutionContext.Run(ExecutionContext executionContext, ContextCallback callback, Object
state, Boolean preserveSyncCtx)
  at System.Threading.ExecutionContext.Run(ExecutionContext executionContext, ContextCallback callback, Object
state)
  at System.Threading.ThreadHelper.ThreadStart()

Work Log:
Starting carving using LimeFrostSearchCarvedHunter
Hunter LimeFrostSearchCarvedHunter took 00:00:00.00 to carve
Starting carving using YahooMessengerHunter
Hunter YahooMessengerHunter took 00:00:00.00 to carve
Starting carving using CarvedPictureHunter
Hunter CarvedPictureHunter took 00:00:00.06 to carve
Starting carving using SpeexAudioPacketHunter
Hunter SpeexAudioPacketHunter took 00:00:00.00 to carve
Starting carving using AvcSequenceHunter
Hunter AvcSequenceHunter took 00:00:00.00 to carve
Starting carving using CarvedVideosHunter

Data Processor #3 timeout info:
```

```
------------------------------------------------------------
Current search item: Data Processor 3:  Searching [ROOT]\Windows\MEMORY.DMP at offset 130023424
Timestamp: 08/16/2019 09:12:32
Operating System: Microsoft Windows NT 10.0.17134.0
Product Version: 3.4.1.15164
.NET Version: 4.0.30319.42000
Current Locale: en-US
Number Of Processors: 1
  Processor 0 Name: Intel(R) Core(TM) i7-8700K CPU @ 3.70GHz
  Processor 0 64-bit Ready: True
  Processor 0 Cores: 6
  Processor 0 Logical Processors: 12
Memory Available: 63.94 GB
Stack trace:
  at DiscUtils.Compression.Zlibwapi.UncompressX64(IntPtr Dest, Int32& DestLen, IntPtr Source, Int32 SourceLen)
  at DiscUtils.Compression.Zlibwapi.UncompressX64(IntPtr Dest, Int32& DestLen, IntPtr Source, Int32 SourceLen)
  at DiscUtils.Compression.Zlibwapi.Uncompress(Byte[] Dest, Int32 dstOffset, Int32& DestLen, Byte[] Source, Int32
srcOffset, Int32 SourceLen)
  at DiscUtils.Ewf.EWFStream.ReadChunk(Int32 chunkNo, Byte[] dest, Int32 destOffset)
  at DiscUtils.Ewf.EWFStream.Read(Byte[] buffer, Int32 offset, Int32 count)
  at DiscUtils.SubStream.Read(Byte[] buffer, Int32 offset, Int32 count)
  at DiscUtils.BlockCacheStream.Read(Byte[] buffer, Int32 offset, Int32 count)
  at Magnet.Utilities.Helpers.StreamHelper.ReadFully(Stream stream, Byte[] buffer, Int32 offset, Int32 length)
  at DiscUtils.Ntfs.RawClusterStream.ReadClusters(Int64 startVcn, Int32 count, Byte[] buffer, Int32 offset)
  at DiscUtils.Ntfs.NonResidentDataBuffer.Read(Int64 pos, Byte[] buffer, Int32 offset, Int32 count)
  at DiscUtils.Ntfs.NtfsAttributeBuffer.Read(Int64 pos, Byte[] buffer, Int32 offset, Int32 count)
  at DiscUtils.BufferStream.Read(Byte[] buffer, Int32 offset, Int32 count)
  at DiscUtils.Ntfs.NtfsFileStream.Read(Byte[] buffer, Int32 offset, Int32 count)
  at DiscUtils.SparseStreamLocked.Read(Byte[] buffer, Int32 offset, Int32 count)
  at DiscUtils.ThreadSafeStream.Read(Byte[] buffer, Int32 offset, Int32 count)
  at Magnet.Engine.Features.Searchable.SubStream.ReadInnerStream(Byte[] buffer, Int32 bufferOffset, Int32
readCount, Int64 streamReadPosition)
  at Magnet.Engine.Features.Searchable.SubStream.UpdateCache(Int64 startOffset, Int64 count)
  at Magnet.Engine.Features.Searchable.SubStream.Read(Byte[] buffer, Int32 offset, Int32 count)
  at Magnet.Artifacts.WindowsPrefetchFiles.WindowsPrefetchFileParser.ParseVolumeNameSection(UInt32
headOffset, Int32 sectionNumber)
  at Magnet.Artifacts.WindowsPrefetchFiles.WindowsPrefetchFileParser.ParseSectionD()
  at Magnet.Artifacts.WindowsPrefetchFiles.WindowsPrefetchFileParser.ParseWin7()
  at Magnet.Artifacts.WindowsPrefetchFiles.WindowsPrefetchFileParser.Parse()
  at Magnet.Artifacts.WindowsPrefetchFiles.WindowsXpVista7PrefetchFilesHunter.<Process>d__8.MoveNext()
  at Magnet.Artifacts.Common.Hunters.Hunter.Hunt(IContext context, CancellationToken cancellationToken)
  at Magnet.Engine.Features.ArtifactEngine.<>c__DisplayClass54_2.<HandlePatternMatches>b__1()
  at Magnet.Engine.Features.ArtifactEngine.<>c__DisplayClass57_0`1.<TryWithEnhancedLogging>b__0()
  at Magnet.Utilities.Exceptions.Try.InReleaseMode[T](Func`1 dangerous)
  at Magnet.Engine.Features.ArtifactEngine.HandlePatternMatches(ICarvedHunter hunter, IEnumerable`1
matches)
  at
Magnet.Engine.Features.ArtifactEngine.<>c__DisplayClass53_0.<HandlePatternMatchesGenerator>b__0(IEnumera
ble`1 matches, CancellationToken token)
  at Magnet.Matching.SinglePass.ByteScanner`1.RunDeferredCallbacks()
  at Magnet.Matching.SinglePass.PfacNative.PfacNativeByteScanner`1.Scan(Int32 startIdx, Int32 maxNumBytes)
  at Magnet.Engine.Features.ArtifactEngine.<>c__DisplayClass58_0.<TryWithEnhancedLogging>b__0()
  at Magnet.Utilities.Exceptions.Try.InReleaseMode(Action dangerous)
```

```
   at Magnet.Engine.Features.ArtifactEngine.SinglePassByteCarve(IEngineSearchable searchable, Int32 startOffset,
IWorkerInformation workerInformation)
   at Magnet.Engine.Features.ArtifactEngine.Carve(IEngineSearchable searchable, IReadOnlyCollection`1
huntStatuses, Int32 startOffset, IWorkerInformation workerInformation, IPerformanceMetrics
performanceMetrics, ManualResetEvent pauseTrigger)
   at Magnet.Engine.Common.Multithreading.CarvedWorkItem.DoWork(IArtifactEngine artifactEngine,
IWorkerInformation workerInformation, IPlatformTranslator platformTranslator, ManualResetEvent pauseTrigger)
   at Magnet.Engine.Common.Multithreading.WorkerThread.ProcessWorkItem(IWorkItem workItem, ICaseWriter
caseWriter, IArtifactEngine engine)
   at Magnet.Engine.Common.Multithreading.WorkerThread.DoWork()
   at System.Threading.ExecutionContext.RunInternal(ExecutionContext executionContext, ContextCallback
callback, Object state, Boolean preserveSyncCtx)
   at System.Threading.ExecutionContext.Run(ExecutionContext executionContext, ContextCallback callback, Object
state, Boolean preserveSyncCtx)
   at System.Threading.ExecutionContext.Run(ExecutionContext executionContext, ContextCallback callback, Object
state)
   at System.Threading.ThreadHelper.ThreadStart()

Work Log:
Starting carving using LimeFrostSearchCarvedHunter
Hunter LimeFrostSearchCarvedHunter took 00:00:00.00 to carve
Starting carving using Skype4xCarvedHunter
Hunter Skype4xCarvedHunter took 00:00:00.00 to carve
Starting carving using Skype5x6xCarvedHunter
Hunter Skype5x6xCarvedHunter took 00:00:00.00 to carve
Starting carving using CarvedPictureHunter
Hunter CarvedPictureHunter took 00:00:00.00 to carve
Starting carving using YahooMessengerHunter
Hunter YahooMessengerHunter took 00:00:00.00 to carve
Starting carving using SpeexAudioPacketHunter
Hunter SpeexAudioPacketHunter took 00:00:00.00 to carve
Starting carving using AvcSequenceHunter
Hunter AvcSequenceHunter took 00:00:00.00 to carve
Starting carving using Vp6Hunter
Hunter Vp6Hunter took 00:00:00.00 to carve
Starting carving using SearchKeywordsHunter
Hunter SearchKeywordsHunter took 00:00:00.00 to carve
Starting carving using CarvedVideosHunter
Hunter CarvedVideosHunter took 00:00:00.00 to carve
Starting carving using CompoundFileCarvingHunter
Hunter CompoundFileCarvingHunter took 00:00:00.00 to carve
Starting carving using CompoundFileCarvingHunter
Hunter CompoundFileCarvingHunter took 00:00:00.00 to carve
Starting carving using CompoundFileCarvingHunter
Hunter CompoundFileCarvingHunter took 00:00:00.00 to carve
Starting carving using WindowsXpVista7PrefetchFilesHunter
```