Evidence Report for Project: Cr06

Project Number: 20171029 06

Project Description:

Image Files:

Disks:
Disk Name: PhysicalDrive1 [USB]

Time Zone Information:

Time Zone: (GMT) Casablanca, Monrovia (Greenwich Standard Time)
Daylight savings (summertime) was in effect: No
Time Zone information obtained from preferences settings.

Total Drive Information

Hard disk make: Virtual HD
Total Sectors : 10485760
Total Size : 5242880 KB

Hard Disk: E:
Drive Type: DRIVE_FIXED
Volume Name: USB
Volume Serial Number : D8C6-150A
File System: NTFS
Bytes Per Sector: 512
Total Clusters: 1309951
Sectors per cluster: 8
Total Sectors: 10479615
Hidden Sectors: 2048
Total Capacity: 5239807 KB
Start Sector: 2048
End Sector: 10481663

Evidence of Interest:

Total Evidence Items of Interest: 3

PhysicalDrive1 Hard Disk E:
List of Files:

PhysicalDrive1\E:\$RECYCLE.BIN\S-1-5-21-418395916-951492369-3763300230-500\desktop.ini
MD5 Checksum: A526B9E7C716B3489D8CC062FBCE4005
Created:05/03/2016 14:20Modified:05/03/2016 14:20Last Accessed:05/03/2016 14:20

ACL Information :

Owner :S-1-5-32-544 BUILTIN\Administrators

Group :S-1-5-21-418395916-951492369-3763300230-513 PLABWIN810\None

S-1-16-4096 Mandatory Label\Low Mandatory Level
[FILE READ]

Audit :S-1-5-32-544 BUILTIN\Administrators
[FILE READ]
[FILE WRITE] [APPEND DATA][READ EXTENDED ATTRIBUTES]
[WRITE EXTENDED ATTRIBUTES] [FILE EXECUTE] [FILE READ ATTRIBUTES]
[FILE WRITE ATTRIBUTES] [FILE DELETE CHILD] [DELETE]
[READ CONTROL] [WRITE DAC] [WRITE OWNER]
[SYNCHRONIZE] [STANDARD RIGHTS REQUIRED]

Permissions:S-1-5-18 NT AUTHORITY\SYSTEM
[FILE READ]
[FILE WRITE] [APPEND DATA][READ EXTENDED ATTRIBUTES]
[WRITE EXTENDED ATTRIBUTES] [FILE EXECUTE] [FILE READ ATTRIBUTES]
[FILE WRITE ATTRIBUTES] [FILE DELETE CHILD] [DELETE]
[READ CONTROL] [WRITE DAC] [WRITE OWNER]
[SYNCHRONIZE] [STANDARD RIGHTS REQUIRED]

Permissions:S-1-5-21-418395916-951492369-3763300230-500 PLABWIN810\Administrator
[FILE READ]
[FILE WRITE] [APPEND DATA][READ EXTENDED ATTRIBUTES]
[WRITE EXTENDED ATTRIBUTES] [FILE EXECUTE] [FILE READ ATTRIBUTES]
[FILE WRITE ATTRIBUTES] [FILE DELETE CHILD] [DELETE]
[READ CONTROL] [WRITE DAC] [WRITE OWNER]
[SYNCHRONIZE] [STANDARD RIGHTS REQUIRED]

PhysicalDrive1\E:\$RECYCLE.BIN\S-1-5-21-497532071-411011935-5816648-500\desktop.ini
MD5 Checksum: A526B9E7C716B3489D8CC062FBCE4005
Created:05/03/2016 10:01Modified:05/03/2016 10:01Last Accessed:05/03/2016 10:01

ACL Information :

Owner :S-1-5-32-544 BUILTIN\Administrators

Group :S-1-5-21-497532071-411011935-5816648-513

S-1-16-4096 Mandatory Label\Low Mandatory Level
[FILE READ]

Audit :S-1-5-32-544 BUILTIN\Administrators
[FILE READ]
[FILE WRITE] [APPEND DATA][READ EXTENDED ATTRIBUTES]
[WRITE EXTENDED ATTRIBUTES] [FILE EXECUTE] [FILE READ ATTRIBUTES]
[FILE WRITE ATTRIBUTES] [FILE DELETE CHILD] [DELETE]
[READ CONTROL] [WRITE DAC] [WRITE OWNER]

[SYNCHRONIZE] [STANDARD RIGHTS REQUIRED]

Permissions:S-1-5-18 NT AUTHORITY\SYSTEM
[FILE READ]
[FILE WRITE] [APPEND DATA][READ EXTENDED ATTRIBUTES]
[WRITE EXTENDED ATTRIBUTES] [FILE EXECUTE] [FILE READ ATTRIBUTES]
[FILE WRITE ATTRIBUTES] [FILE DELETE CHILD] [DELETE]
[READ CONTROL] [WRITE DAC] [WRITE OWNER]
[SYNCHRONIZE] [STANDARD RIGHTS REQUIRED]

Permissions:S-1-5-21-497532071-411011935-5816648-500
[FILE READ]
[FILE WRITE] [APPEND DATA][READ EXTENDED ATTRIBUTES]
[WRITE EXTENDED ATTRIBUTES] [FILE EXECUTE] [FILE READ ATTRIBUTES]
[FILE WRITE ATTRIBUTES] [FILE DELETE CHILD] [DELETE]
[READ CONTROL] [WRITE DAC] [WRITE OWNER]
[SYNCHRONIZE] [STANDARD RIGHTS REQUIRED]

PhysicalDrive1\E:\System Volume Information\tracking.log
MD5 Checksum: 8B1C3CA184A90391FFB995017129DC5C
Created:05/03/2016 14:16Modified:05/04/2016 11:31Last Accessed:05/03/2016 14:16

ACL Information :

Owner :S-1-5-18 NT AUTHORITY\SYSTEM

Group :S-1-5-18 NT AUTHORITY\SYSTEM

Audit :S-1-5-32-544 BUILTIN\Administrators
[FILE READ]
[FILE WRITE] [APPEND DATA][READ EXTENDED ATTRIBUTES]
[WRITE EXTENDED ATTRIBUTES] [FILE EXECUTE] [FILE READ ATTRIBUTES]
[FILE WRITE ATTRIBUTES] [FILE DELETE CHILD] [DELETE]
[READ CONTROL] [WRITE DAC] [WRITE OWNER]
[SYNCHRONIZE] [STANDARD RIGHTS REQUIRED]

Permissions:S-1-5-18 NT AUTHORITY\SYSTEM
[FILE READ]
[FILE WRITE] [APPEND DATA][READ EXTENDED ATTRIBUTES]
[WRITE EXTENDED ATTRIBUTES] [FILE EXECUTE] [FILE READ ATTRIBUTES]
[FILE WRITE ATTRIBUTES] [FILE DELETE CHILD] [DELETE]
[READ CONTROL] [WRITE DAC] [WRITE OWNER]
[SYNCHRONIZE] [STANDARD RIGHTS REQUIRED]

PhysicalDrive1 Hard Disk E: : **Evidence of Interest:** 3

Clusters of Interest:

File Signature Mismatch:

Registry Keys of Interest:

Event Log Entries of Interest:

Internet Activity Information:

Search Results:

Project Notes:

This Report was created by Aydın Keskin