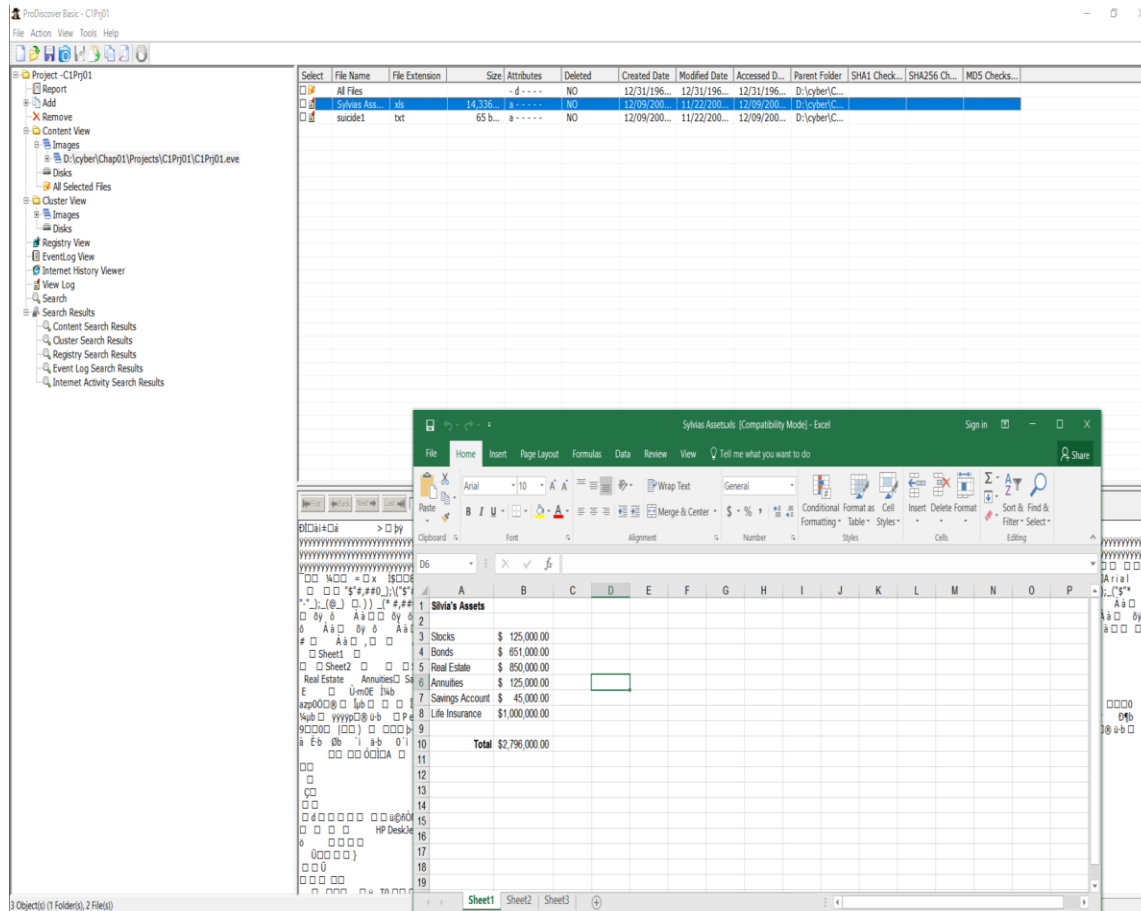


2017-02-27

## Crime91.460-530.203 Cyber Crime Investigation

## Assignment 2: Chapter 1 (10 points)

**Hands-on project 1-1: Provide a screenshot for Step 7.**



## Hands-on project 1-2: Provide a screenshot for Step 8.

ProDiscover Basic - C1Prj02

File Action View Tools Help

Project - C1Prj02

- Report
- Add
- Remove
- Content View
  - Images
  - D:\cyber\Chap01\Projects\C1Prj02.eve
  - Disks
  - All Selected Files
- Cluster View
  - Images
  - Disks
- Registry View
- EventLog View
- Internet History Viewer
- View Log
- Search
  - Search Results
  - Content Search Results
  - Cluster Search Results
  - Registry Search Results
  - Event Log Search Results
  - Internet Activity Search Results

Search 1

Search terms: All Patterns Add to Export Patterns Selection Filter

Select	Cluster Number	Found in	MD5 Checksum	SHA1 Checksum	SHA256 Checksum
<input type="checkbox"/>	166 (858)	D:\cyber\Chap01\Projects\C1Prj02.eve	3b1186a2b3e3d2465050a4155e455		
<input type="checkbox"/>	197 (407)	D:\cyber\Chap01\Projects\C1Prj02.eve	09db8e7db2e5d5f5e6b6dede6d87896		
<input type="checkbox"/>	151A1 (86433)	D:\cyber\Chap01\Projects\C1Prj02.eve	2da9e47d5d8c75523acc59b7a178e60		
<input type="checkbox"/>	151E6 (86502)	D:\cyber\Chap01\Projects\C1Prj02.eve	70a6547a37600c21d84ba1db50633		
<input type="checkbox"/>	152C0 (86572)	D:\cyber\Chap01\Projects\C1Prj02.eve	dac2358c8f04ac3792ca0446e802a		
<input type="checkbox"/>	152D0 (86653)	D:\cyber\Chap01\Projects\C1Prj02.eve	6e409462a4e05a07713eeed9b1489		
<input type="checkbox"/>	15305 (86789)	D:\cyber\Chap01\Projects\C1Prj02.eve	d8b5811dad71e5a7d1427655963a		
<input type="checkbox"/>	15353 (86867)	D:\cyber\Chap01\Projects\C1Prj02.eve	ddd8e67dad95155dbbe86c1506edc		
<input type="checkbox"/>	1538C (86924)	D:\cyber\Chap01\Projects\C1Prj02.eve	245453737b01202391cbe650763153a		
<input type="checkbox"/>	153C5 (86981)	D:\cyber\Chap01\Projects\C1Prj02.eve	a6a8ec03a46e3c10acdb959d9c4d72c		
<input type="checkbox"/>	15425 (87077)	D:\cyber\Chap01\Projects\C1Prj02.eve	3a68c9a9cc2952ba106e94d99537e		
<input type="checkbox"/>	1543D (87171)	D:\cyber\Chap01\Projects\C1Prj02.eve	c26c7ba574986031d3baa4d77796b		
<input type="checkbox"/>	154E1 (87265)	D:\cyber\Chap01\Projects\C1Prj02.eve	c1956196a08f1c1af236a9aband79d		
<input type="checkbox"/>	15544 (87364)	D:\cyber\Chap01\Projects\C1Prj02.eve	b7b08652db18128c54e4b1bf1a4559		
<input type="checkbox"/>	15590 (87440)	D:\cyber\Chap01\Projects\C1Prj02.eve	76519165a9eb44acbb802b38b5adcf5		
<input type="checkbox"/>	155D7 (87511)	D:\cyber\Chap01\Projects\C1Prj02.eve	71372b4e699d7822818db70a768882		
<input type="checkbox"/>	15630 (87600)	D:\cyber\Chap01\Projects\C1Prj02.eve	6198af9e48bcb8652b03de42211a77		
<input type="checkbox"/>	1568A (87690)	D:\cyber\Chap01\Projects\C1Prj02.eve	752b7207040a633db6c52a521069d8		
<input type="checkbox"/>	156D6 (87766)	D:\cyber\Chap01\Projects\C1Prj02.eve	87e53d8711a75411136bd51c5a87013		
<input type="checkbox"/>	15738 (87864)	D:\cyber\Chap01\Projects\C1Prj02.eve	1489798521cc46a0a5d8974991770e		
<input type="checkbox"/>	1577F (87936)	D:\cyber\Chap01\Projects\C1Prj02.eve	db80caa70ad9db9963194d026c5d5		
<input type="checkbox"/>	157E3 (88035)	D:\cyber\Chap01\Projects\C1Prj02.eve	40b0c4f40a6d579e07a8272949b814		
<input type="checkbox"/>	15825 (88101)	D:\cyber\Chap01\Projects\C1Prj02.eve	9e98016e722d614a9565679ea12156		
<input type="checkbox"/>	1586D (88173)	D:\cyber\Chap01\Projects\C1Prj02.eve	6109c4b02a7dbab76a3279d173bbac		
<input type="checkbox"/>	1588B (88251)	D:\cyber\Chap01\Projects\C1Prj02.eve	4f5cdd000c9789638885b0ea383		
<input type="checkbox"/>	158E7 (88296)	D:\cyber\Chap01\Projects\C1Prj02.eve	78f123102751a303a7021870c053a3f		
<input type="checkbox"/>	158F9 (88313)	D:\cyber\Chap01\Projects\C1Prj02.eve	0ba003300020077014ba34c5996d514		

For Help, press F1

MD5

## Hands-on project 1-3: Follow the instruction and complete Step 9.

I followed the steps listed in the book. I check all the files in C1Prj03.dd and under English/Rights/ Economic Indicators\_gov\_files/footer\_files, I found the GIF which shows the number 461562.

### **Evidence Report for Project:** C1Prj03

**Project Number:** 20170227

#### **Project Description:**

##### **Image Files:**

**File Name:** D:\cyber\Chap01\Projects\C1Prj03.dd

Image File Type: DFT Image

File Number: Unknown

Technician Name: Unknown

Date: 00/00/00

Time: 00:00:00

MD5 Checksum:

Checksum Validated: No

Compressed image: No

##### **Time Zone Information:**

Time Zone: (GMT-05:00) Bogota, Lima, Quito (SA Pacific Standard Time)

Daylight savings (summertime) was in effect: No

Time Zone information obtained from preferences settings.

Hard Disk: D:\cyber\Chap01\Projects\C1Prj03.dd

Volume Name: NO NAME

Volume Serial Number : FC6E-155B

File System: FAT32

Bytes Per Sector: 512

Total Clusters: 125972

Sectors per cluster: 2

Total Sectors: 253952

Hidden Sectors: 0

Total Capacity: 126976 KB

Start Sector: 0

End Sector: 253951

#### **Disks:**

#### **Evidence of Interest:**

Total Evidence Items of Interest: 1

Hard Disk: Unknown

List of Files:

D:\cyber\Chap01\Projects\C1Prj03.dd\English\Rights\Economic  
Indicators\_gov\_files/footer\_files\COUNT.GIF

MD5 Checksum: CEC7BACC70B3E8950CC019D287B72CC8

Created:07/30/2006 18:40:52Modified:07/30/2006 18:40:54Last

Accessed:07/30/2006 00:00:00

#### **Cluster Chain:**

Start Cluster	End Cluster	Total Clusters
89805 (15ECD)	89805 (15ECD)	1
<a href="#">Investigator's comments:</a> 461562		

---

D:\cyber\Chap01\Projects\C1Prj03.dd Hard Disk Unknown : **Evidence of Interest:** 1

**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 ProDiscover**

**Hands-on project 1-6: Follow Step 5 and paste the report here or submit the report as standalone file in pdf or doc.**

**Evidence Report for Project:** C1Prj06

**Project Number:** 20170227

**Project Description:**

**Image Files:**

**File Name:** D:\cyber\Chap01\Projects\C1Prj06.eve

Image File Type: DFT Image

File Number: C2Proj06

Technician Name: Joe Friday

Date: 09/24/2006

Time: 21:57:21

MD5 Checksum: a36e6382b99447726e8466951093bfeb

Checksum Validated: No

Compressed image: No

**Time Zone Information:**

Time Zone: (GMT-08:00) Pacific Time (US & Canada); Tijuana (Pacific Standard Time)  
Daylight savings (summertime) was in effect: Yes  
Time Zone information obtained automatically from remote system/image.

Hard Disk: D:\cyber\Chap01\Projects\C1Prj06.eve

Volume Name:  
File System: FAT12  
Bytes Per Sector: 512  
Total Clusters: 2847  
Sectors per cluster: 1  
Total Sectors: 2880  
Hidden Sectors: 0  
Total Capacity: 1440 KB  
Start Sector: 0  
End Sector: 2879

### Disks:

### Evidence of Interest:

Total Evidence Items of Interest: 3

Hard Disk: A:\  
List of Files:

D:\cyber\Chap01\Projects\C1Prj06.eve\The Tragedy of Hamlet.doc

MD5 Checksum: 0EC248046D7663CAF9B5ED8F2D71295B

Deleted: Deleted: 06/24/2004 00:00:00

#### Cluster Chain:

Start Cluster	End Cluster	Total Clusters
---------------	-------------	----------------

Investigator's comments: HAS KEYWORDS

---

D:\cyber\Chap01\Projects\C1Prj06.eve\The Merry Wives of Windsor.doc

MD5 Checksum: 2DE33CCA01F04CE4811335072BF23736

Created:06/23/2004 22:40:26Modified:06/23/2004 21:24:40Last

Accessed:06/23/2004 00:00:00

#### Cluster Chain:

Start Cluster	End Cluster	Total Clusters
---------------	-------------	----------------

605 (25D)	925 (39D)	321
-----------	-----------	-----

Investigator's comments: HAS KEYWORD

---

D:\cyber\Chap01\Projects\C1Prj06.eve\The Merchant of Venice.doc

MD5 Checksum: D524CEA951FB29125300A56D3CD4CF91

Created:06/23/2004 22:40:22Modified:06/23/2004 21:25:20Last

Accessed:06/24/2004 00:00:00

#### Cluster Chain:

Start Cluster	End Cluster	Total Clusters
---------------	-------------	----------------

463 (1CF)

604 (25C)

142

Investigator's comments: HAS KEYWORD

---

---

D:\cyber\Chap01\Projects\C1Prj06.eve Hard Disk A:\ : **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 ProDiscover**