

## Examination Notes

Examination Number: 2

Examiner Name: Akshay Chaurasia

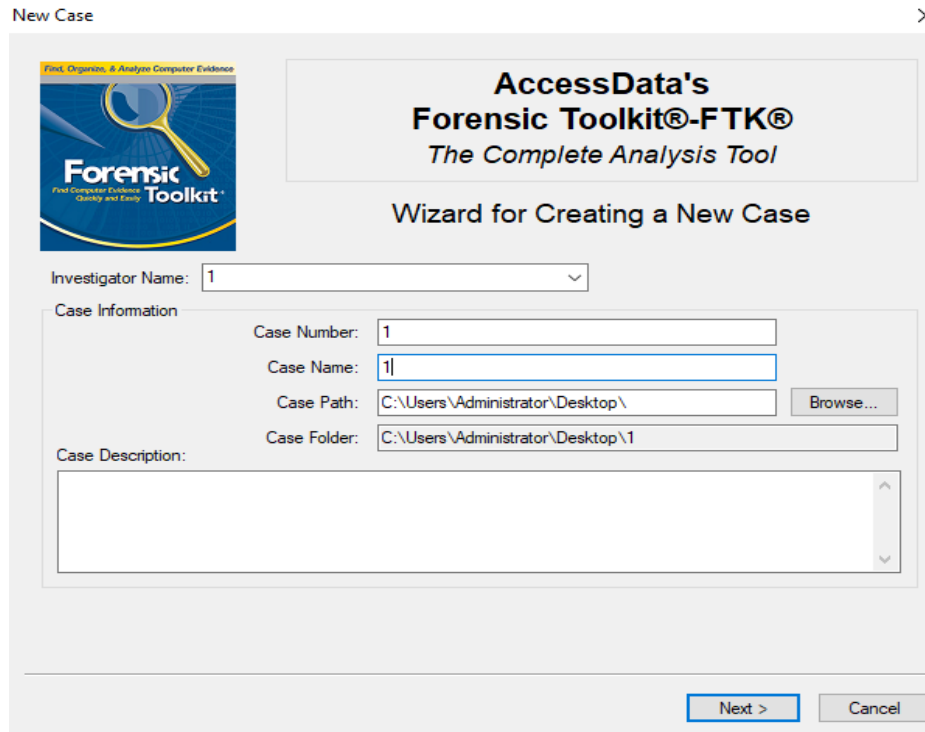
Date & Time

Activity

10/13/2019  
2:10 PM

The corporate provided a **.zip** file containing the registry files from Mark's computer and the imaged USB in EnCase (**.eo1**)

I started examining the image file of the USB provided by the corporate using the Forensic Toolkit (FTK)



## Examination Notes

Examination Number: 2

Examiner Name: Akshay Chaurasia

10/13/2019  
2:15 PM

Case Log Options

### Case Log Options

The case log is a text file named FTK.log in the case folder. It gets created automatically by FTK and contains a record of events that occur during the course of the case. You can choose which type of events you would like to be logged.

You can also add your own comments to the log file at any time by selecting "Add Case Log Entry..." under the "Tools" menu item, and you can view the log file by selecting "View Case Log" under the "Tools" menu item.

Events to go in the Case Log

<input checked="" type="checkbox"/> Case and evidence events	Events related to the addition and processing of file items when evidence is added or when using Analysis Tools later in the case.
<input checked="" type="checkbox"/> Error messages	Events related to any error conditions encountered during the case.
<input checked="" type="checkbox"/> Bookmarking events	Events related to the addition and modification of bookmarks.
<input checked="" type="checkbox"/> Searching events	Events related to searching. All search queries and resulting hit counts will be recorded.
<input checked="" type="checkbox"/> Data carving / Internet searches	Events related to special data carving or internet keyword searches that are performed during the case.
<input checked="" type="checkbox"/> Other events	Other events not related to the above, such as copying, viewing, and ignoring files.

< Back Next > Cancel

2:18 PM

Evidence Processing Options

### Processes to Perform

Evidence is added to a case in several steps. Some of the processes are always performed, while others are optional, depending on your needs and time/resource constraints.

<input checked="" type="checkbox"/> MD5 Hash	An MD5 hash is a 16 byte value generated based upon a file's content. It is used to uniquely identify files. Hashes can be used to verify a file's integrity, or to identify duplicate files. MD5 hashes are used by the KFF to identify known files.
<input checked="" type="checkbox"/> SHA1 Hash	A SHA1 hash is a 20 byte value. The SHA1 hashing algorithm is newer than MD5, but is not yet as widely used.
<input checked="" type="checkbox"/> KFF Lookup	KFF (Known File Filter) is a utility that compares MD5 file hashes against a database of MD5 hashes from known files. The purpose of KFF is to eliminate files known to be unimportant, or to alert the investigator to known illicit or dangerous files.
<input checked="" type="checkbox"/> Entropy Test	For unknown file types, an entropy test is used to determine whether the file's data is compressed or encrypted. Such files contain no plain text and will not be indexed. Unnecessary indexing of such files can waste large amounts of time and resources.
<input checked="" type="checkbox"/> Full Text Index	The Forensic Toolkit includes a very powerful search engine, dtSearch, which enables the investigator to do instantaneous searching of textual data. In order to take advantage of this search feature, the data must first be indexed.
<input checked="" type="checkbox"/> Store Thumbnails	Create and store thumbnails for all graphics in the case. This option speeds up browsing through the Graphics view at the expense of consuming more space in the case folder.
<input checked="" type="checkbox"/> Decrypt EFS Files	Automatically locate and attempt to decrypt EFS encrypted files found on NTFS partitions within the case. (Requires AccessData Password Recovery Toolkit 5.20 or newer)
<input checked="" type="checkbox"/> File Listing Database	Create a Microsoft Access (Jet) database containing a list of all files in the case. The attributes included are based on the Preprocessing File Listing Database Column Setting. This database can be recreated with custom column settings in Copy Special.
<input type="checkbox"/> HTML File Listing	Create an HTML version of the File Listing.
<input type="checkbox"/> Data Carve	Automatically find specific file types embedded in other files and from free space. Retrieve results using Data Carving Option on Tools Menu. <a href="#">Carving Options</a>
<input type="checkbox"/> Registry Reports	Generate common registry reports during preprocessing.

< Back Next > Cancel

2:25 PM

Refine Case - Default

### Refine Case - Default

In order to save time and resources, and/or to eliminate irrelevant data, you may choose to exclude certain kinds of data from the case. Here, you can choose default inclusion/exclusion settings that will apply to each evidence item that gets added to the case. To exclude data, make any changes to the settings below. Note: any items that get excluded will not appear anywhere in the case, and will be inaccessible.

**Include All Items** | Optimal Settings | Email Emphasis | Text Emphasis | Graphics Emphasis

Unconditionally Add

- ☒ File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)
- ☒ Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)
- ☒ KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e., OS system files, known applications, etc.)
- ☐ Extract files from KFF ignorable containers

Conditionally Add

Add other items to the case only if they satisfy **BOTH the file status and the file type** criteria

File Status Criteria			File Type Criteria	
Deletion Status:	Encryption Status:	Email Status:	<input checked="" type="checkbox"/> Documents	<input checked="" type="checkbox"/> Executables
<input type="radio"/> Deleted	<input type="radio"/> Encrypted	<input type="radio"/> From email	<input checked="" type="checkbox"/> Spreadsheets	<input checked="" type="checkbox"/> Archives
<input type="radio"/> Not deleted	<input type="radio"/> Not encrypted	<input type="radio"/> Not from email	<input checked="" type="checkbox"/> Databases	<input checked="" type="checkbox"/> Folders
<input checked="" type="radio"/> Either	<input checked="" type="radio"/> Either	<input checked="" type="radio"/> Either	<input checked="" type="checkbox"/> Graphics	<input checked="" type="checkbox"/> Other Known
<input checked="" type="checkbox"/> Include Duplicate Files		<input checked="" type="checkbox"/> OLE Streams	<input checked="" type="checkbox"/> Multimedia	<input checked="" type="checkbox"/> Unknown
			<input checked="" type="checkbox"/> Email msgs	

< Back | Next > | Cancel

Refine Index - Default

### Refine Index - Default

In order to save time and resources, and/or to make searching more efficient, you may choose to exclude certain kinds of data from being indexed. Here, you can choose default settings that will apply to each evidence item that gets added to the case. To exclude items from being indexed, make any changes to the settings below. Note: any items that don't get indexed initially can be indexed later by clicking on "Analysis Tools" under the "Tools" menu item.

Unconditionally Index

- ☒ File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)
- ☒ Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)
- ☐ KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e., OS system files, known applications, etc.)

Conditionally Index

Index other items in the case only if they satisfy **BOTH the file status and the file type** criteria

File Status Criteria			File Type Criteria	
Deletion Status:	Encryption Status:	Email Status:	<input checked="" type="checkbox"/> Documents	<input checked="" type="checkbox"/> Executables
<input type="radio"/> Deleted	<input type="radio"/> Encrypted	<input type="radio"/> From email	<input checked="" type="checkbox"/> Spreadsheets	<input checked="" type="checkbox"/> Archives
<input type="radio"/> Not deleted	<input type="radio"/> Not encrypted	<input type="radio"/> Not from email	<input checked="" type="checkbox"/> Databases	<input checked="" type="checkbox"/> Folders
<input checked="" type="radio"/> Either	<input checked="" type="radio"/> Either	<input checked="" type="radio"/> Either	<input checked="" type="checkbox"/> Graphics	<input checked="" type="checkbox"/> Other Known
<input checked="" type="checkbox"/> Include Duplicate Files		<input checked="" type="checkbox"/> OLE Streams	<input checked="" type="checkbox"/> Multimedia	<input checked="" type="checkbox"/> Unknown
			<input checked="" type="checkbox"/> Email msgs	

< Back | Next > | Cancel

## Examination Notes

Examination Number: 2

Examiner Name: Akshay Chaurasia

2:30 PM

2:34 PM

Add Evidence to Case

### Add Evidence

Any number of evidence items can be added to the case. There are several types of evidence items:

- Acquired image of drive: Several formats supported; can be an image of a logical or physical drive
- Local drive: Can be a logical or physical drive
- Folder: Adds all files in the specified folder, including contents of subfolders
- Individual File: Adds a single file. NOTE: Disk image files should be added as acquired images.

The default refinement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specific folders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced...

Add Evidence... Edit Evidence... Remove Evidence Refine Evidence - Advanced...

Display Name	Source	Name/Nu...	Type	Refined	Time Zone	Comment
NTUSER	C:\Users\Adm...		Individual f...	N	N/A	
SAM	C:\Users\Adm...		Individual f...	N	N/A	
SECURITY	C:\Users\Adm...		Individual f...	N	N/A	
software	C:\Users\Adm...		Individual f...	N	N/A	
system	C:\Users\Adm...		Individual f...	N	N/A	

< Back Next > Cancel

Loaded the "USB drive image" on FTK.

AccessData FTK 1.81.3 DEMO VERSION

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

Evidence Items: 0

File Items: 0

Total File Items: 0

Checked Items: 0

Unchecked Items: 0

Flagged Thumbnails: 0

Other Thumbnails: 0

Filtered In: 0

Filtered Out: 0

Unfiltered: 0

All Items: 0

File Status

KFF Alert Files: 0

Bookmarked Items: 0

Bad Extension: 0

Encrypted Files: 0

From E-mail: 0

Deleted Files: 0

From Recycle Bin: 0

Duplicate Items: 0

OLE Subitems: 0

Flagged Ignore: 0

File Category

Documents: 0

Spreadsheets: 0

Databases: 0

Graphics: 0

Multimedia: 0

E-mail Messages: 0

Executables: 0

Archives: 0

Folders: 0

Slack/Free Space: 0

Processing Files...

Current Evidence Item:  
C:\Users\Administrator\Desktop\Exam 2\New folder\Lab0607V2\Lab0607V2.E01

Current File Item:  
Lab0607V2\Part\_1\RODGER-FAT32\Thunderbird\Portable\App\thun... \en-US.jar>customize toolbar.properties

Current File Item Status

Action: Reading Data

File Type: 307

Item Size: 307

Progress: 0.00:00:20

Total Process Status

Elapsed Time: 0.00:00:20

Total Items Examined: 843

Total Items Added: 842

Total Items Indexed: 839

Log the case/system status every 10 minutes Log extended information

Cancel

Evidence File Name	Evidence Path	Display Name	Identification Name/Nu...	Evide
--------------------	---------------	--------------	---------------------------	-------

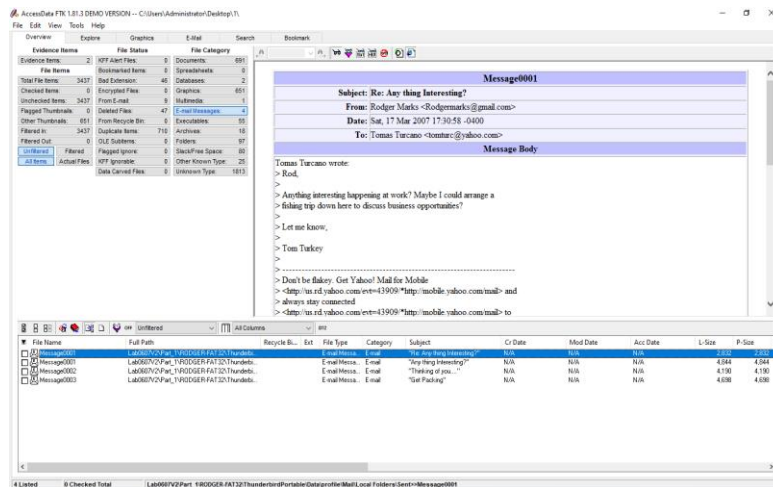
0 Listed 0 Checked Total 0 Highlighted

## Examination Notes

Examination Number: 2

Examiner Name: Akshay Chaurasia

Went to the "Overview" tab of FTK and found out that there were 4 e-mails.



Sorted the emails by date

Unfiltered																								All Columns		DTZ	
v	Idx	Sector	Cluster	Alt Na...	Dup	RO	Sys	H...	Item #	Cmp	KFF	Badkt	Emailed	Header	MD5 Hash	SHA1 Ha...	Hash Set	Email Date	From	To	CC	Attachment Info	BCC				
	Full								1930				Y	3C68746...	EE6A7A25...	C8E5977D...		Fri, 16 Mar 2007 18:1...	Tomas Turca...	Rodger (rod...							
	Full								1913				Y	2550444...	E7477D8E...	009EC2AF...		Sat, 17 Mar 2007 17:...	Rodger Mark...	Tomas Turca...							
	Full								1931				Y	3C68746...	B115C126...	EE938075...		Sat, 17 Mar 2007 21:...	"Sally Smith"...	rodgermarks...							
	Full								1933				Y	3C68746...	E5787E41...	B3A1575E...		Sun, 18 Mar 2007 07:...	Tomas Turca...	Rodger Mark...							

Now, reading the mesaages after sorting it.

## Examination Notes

Examination Number: 2

Examiner Name: Akshay Chaurasia

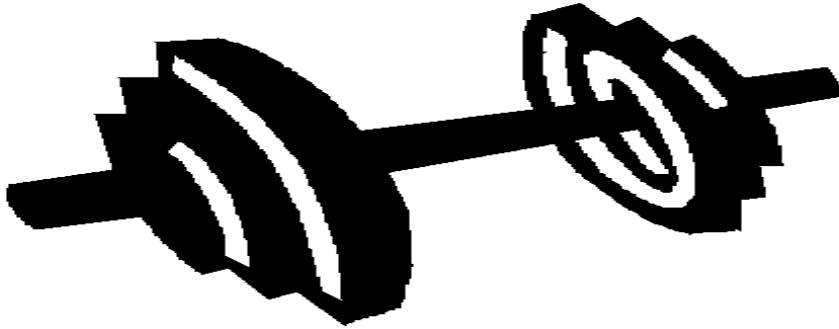
Message0001	
Subject:	Any thing Interesting?
From:	Tomas Turcano <tomturc@yahoo.com>
Date:	Fri, 16 Mar 2007 18:17:38 -0700 (PDT)
To:	Rodger <rodgermarks@gmail.com>
Message Body	
Rod,	
Anything interesting happening at work? Ma ybe I could arrange a fishing trip down here to discuss business opportunit ies?	
Let me know,	
Tom Turkey	
Don't be flakey. <a href="#">Get Yahoo! Mail for Mobile</a> and <a href="#">always st ay connected</a> to friends.	

Main Message Header
From - Fri Mar 16 22:46:22 2007
X-Account-Key: account2
X-UIDL: GmailId1115d78a5596d222
X-Mozilla-Status: 0003
X-Mozilla-Status-2: 00000000

Message0001	
Subject:	Re: Any thing Interesting?
From:	Rodger Marks <Rodgermarks@gmail.com>
Date:	Sat, 17 Mar 2007 17:30:58 -0400
To:	Tomas Turcano <tomturc@yahoo.com>
Message Body	
Tomas Turcano wrote:	
> Rod,	
>	
> Anything interesting happening at work? Maybe I could arrange a	
> fishing trip down here to discuss business opportunities?	
>	
> Let me know,	
>	
> Tom Turkey	
>	
> -----	
> Don't be flakey. Get Yahoo! Mail for Mobile	
> < <a href="http://us.rd.yahoo.com/evt=43909/*http://mobile.yahoo.com/mail">http://us.rd.yahoo.com/evt=43909/*http://mobile.yahoo.com/mail</a> > and	
> always stay connected	
> < <a href="http://us.rd.yahoo.com/evt=43909/*http://mobile.yahoo.com/mail">http://us.rd.yahoo.com/evt=43909/*http://mobile.yahoo.com/mail</a> > to	
> friends.	
Do you think this would be enough for a week of bonefishing?	
Rod	
Attachment	
-----Attachment1-----	
File name = "Top Secret.pdf"	

**Top Secret**

Design of new lipid processor



Cast Iron is the secret ingredient!

**Message0002****Subject:** Thinking of you....**From:** "Sally Smith" <sallysmith645@hotmail.com>**Date:** Sat, 17 Mar 2007 21:43:55 +0000**To:** roddermarks@gmail.com**Message Body**

When I saw this I thought of you. Hope your new venture give us lots of money to enjoy life!

[http://money.cnn.com/magazines/fortune/fortune\\_archive/2007/03/19/8402362/index.htm](http://money.cnn.com/magazines/fortune/fortune_archive/2007/03/19/8402362/index.htm)

Sally

---

i'm making a difference. Make every IM count for the cause of your choice.

Join Now.

<http://clk.atdmt.com/MSN/go/msnkwme0080000001msn/direct/01/?href=http://m.live.com/messenger/im/home/?source=hmtagline>

[http://money.cnn.com/magazines/fortune/fortune\\_archive/2007/03/19/8402362/index.htm](http://money.cnn.com/magazines/fortune/fortune_archive/2007/03/19/8402362/index.htm)

money.cnn.com/magazines/fortune/fortune\_archive/2007/03/19/8402362/index.htm



Companies Markets Tech Media

## The Bachelor meets the Bugatti

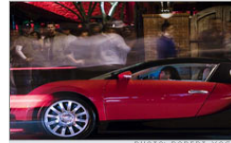
L.A.'s nightlife impresario takes delivery of the most exclusive production car in the world - and invites Fortune's Sue Callaway to help break it in.

By Sue Zesiger Callaway, Fortune  
March 16 2007: 11:14 AM EDT

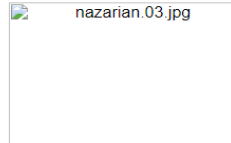
(Fortune Magazine) -- This is about superlatives. A car, the Bugatti Veyron, that is unlike any other production car on the planet. And an entrepreneur, Sam Nazarian, CEO of SBE Entertainment, who is out to transform nightlife as we know it. First things first: the wheels. In a risky corporate move, the VW Group revived the Bugatti marque in 1998 and started down the road to building the ultimate production car - in looks, in technical refinement, in exclusivity. Founder Ettore Bugatti, who died in 1947, became legendary for crafting amazingly advanced high-performance cars that behaved well on the street and were nothing short of art on wheels. His motto: "Nothing is too expensive, nothing is too beautiful." To date, VW's Bugatti has taken 135 orders, and delivered 52 of the 300 Veyrons that will be made. And true to Ettore's vision, the two-seater makes good on all promises, from bespoke componentry to highest-caliber craftsmanship. And cost: \$1.4 million.

I wanted to know who buys such a thing and what it's like to own one. So I hitched a ride with Nazarian, who just took delivery of a gorgeous red and black version. If you don't spend time on the Left Coast, you may not have heard of Nazarian - yet. A son of Qualcomm co-founder Younes Nazarian, Sam is 31, ambitious, and on a tear. He's building a network of high-end restaurants, clubs, real estate developments and hotels designed by Philippe Starck. He also has a movie production company; his latest project, "Mr. Brooks," starring Kevin Costner, Demi Moore, and William Hurt, is due out in June. And he's doing it all with Bugatti speed. (To put that into perspective, the car goes zero to 62 in 2.5 seconds, faster than many current Formula One cars.) "In terms of hotels, I want to build the Four Seasons of our generation - a chic, tasteful experience," he explained. "And I want your room key to give you VIP access to our clubs and restaurants."

Nazarian and I took a Saturday-night tour of his white-hot spots. As we carefully climbed into the low-slung Veyron, he laughed. "It's like high heels - putting them on is tough, but you look great once you're in - or so I've heard." I was engrossed in admiring the machine-turned center console surround, the yards of creamy Austrian leather, the START button calling my name. Alas, Nazarian drove first.



Callaway sits in the Bugatti Veyron, outside The Abbey in West Hollywood



Nazarian (with Callaway) owns L.A. clubs like the Abbey, Area and Hyde.

### Message0003

Subject: Get Packing

From: Tomas Turcano <tomturc@yahoo.com>

Date: Sun, 18 Mar 2007 07:17:14 -0700 (PDT)

To: Rodger Marks <rodgermarks@gmail.com>

### Message Body

I think you earned your fishing trip!

I'll call you at home to arrange.

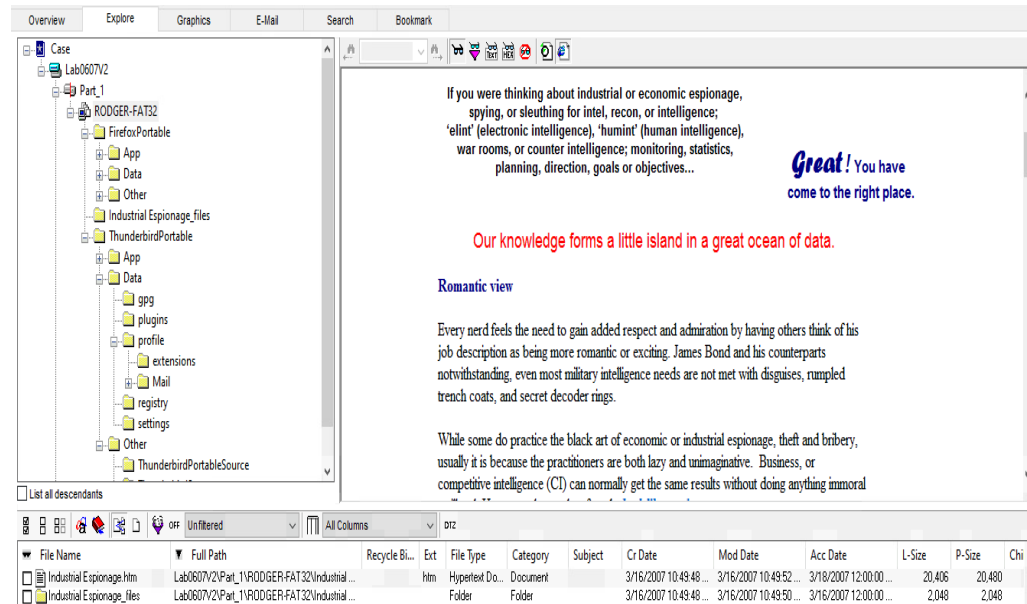
Turkey

8:00? 8:25? 8:40? Find a flick in no time  
with theYahoo! Search movie showtime shortcut.



2:49 PM

In the Explore tab, I also found a .html file names Industrial Espionage.



Then I opened the registry files that were provided to me by the corporate . I opened it using the "Registry Viewer".

In the registry viewer we can see that there were 2 USB drives connected to the computer.

**Examiner Name: Akshay Chaurasia**

Examiner Initials: Akshay Chaurasia