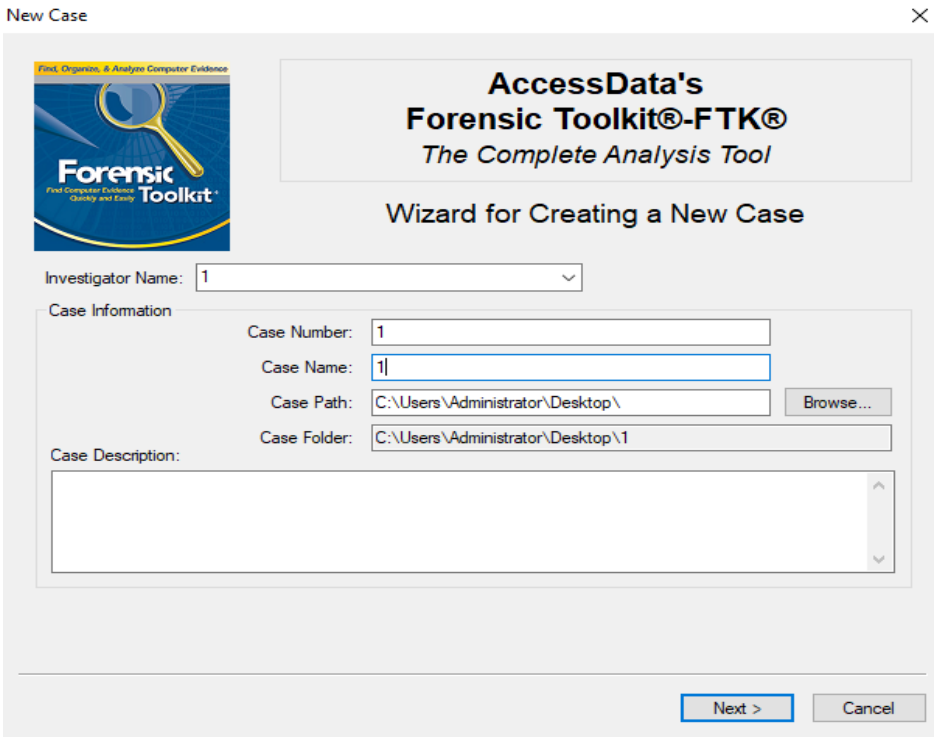
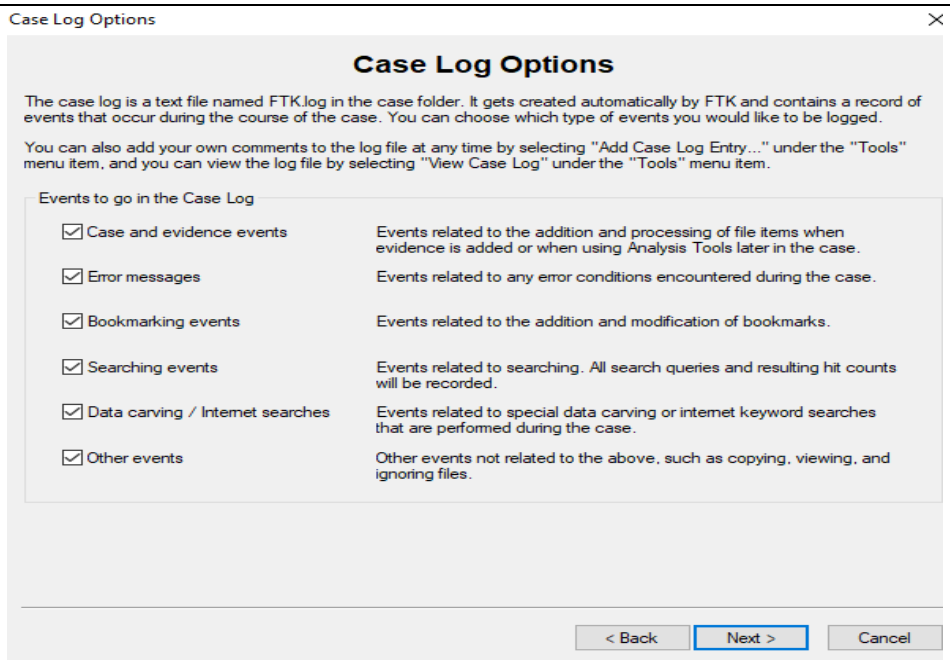
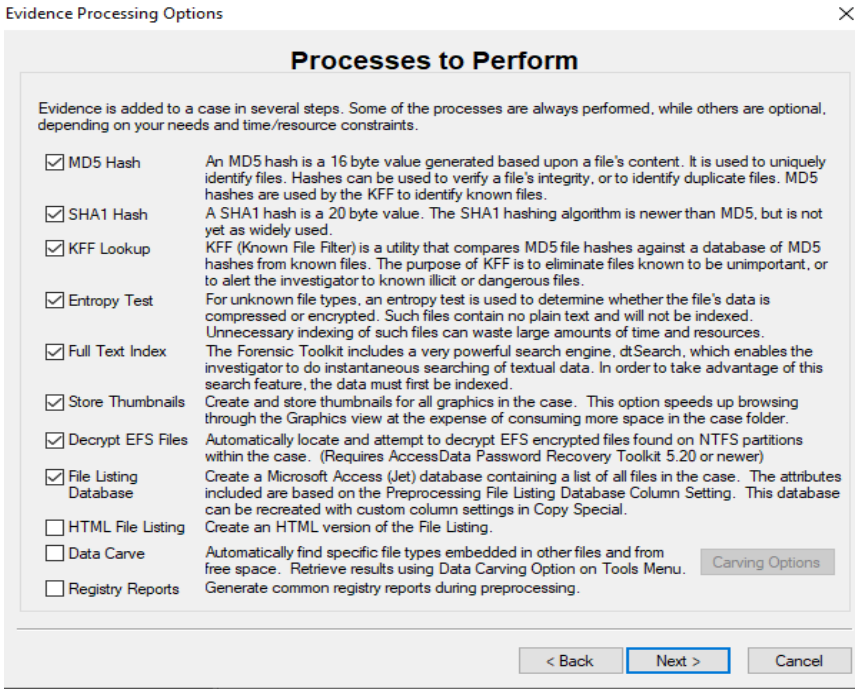
Date & Time	Activity
10/13/2019 2:10 PM	The corporate provided a **.zip** file containing the registry files from Mark's computer and the imaged USB in EnCase **(.eo1)** I started examining the image file of the USB provided by the corporate using the Forensic Toollkit (FTK) 

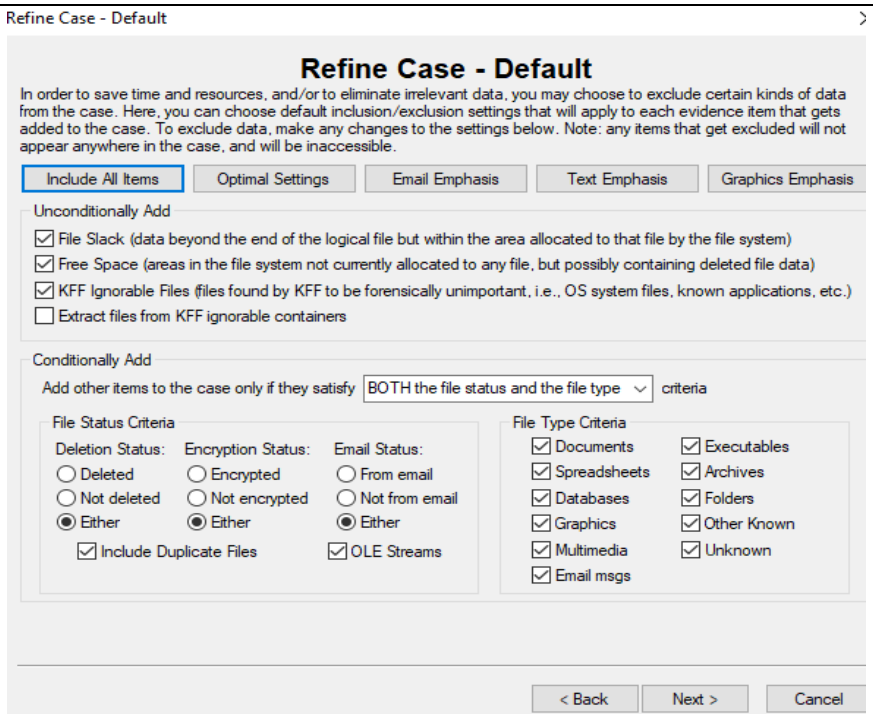
10/13/2019
2:15 PM

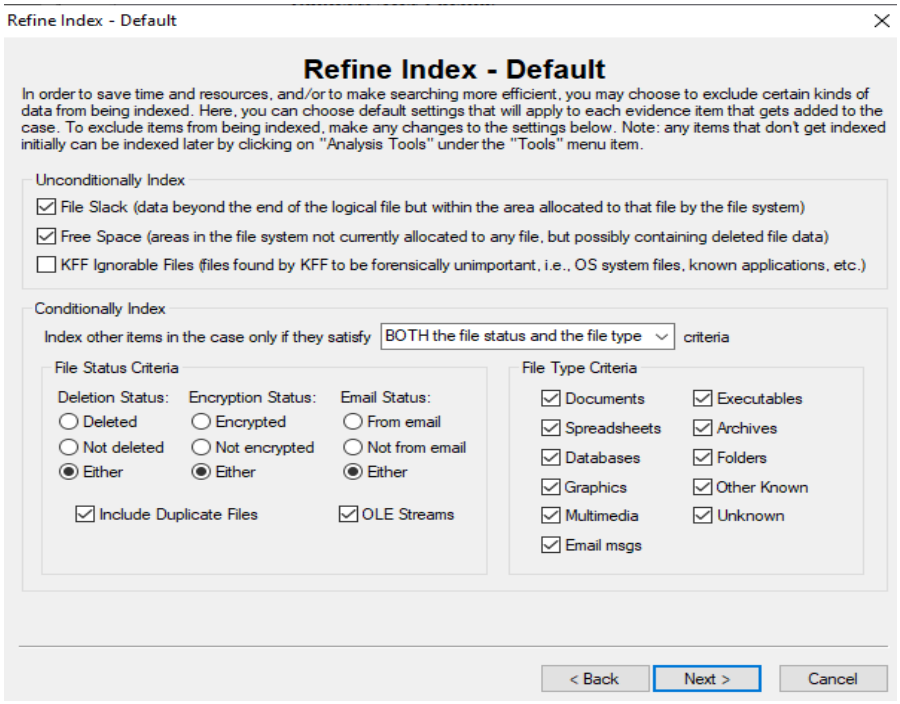


2:18 PM

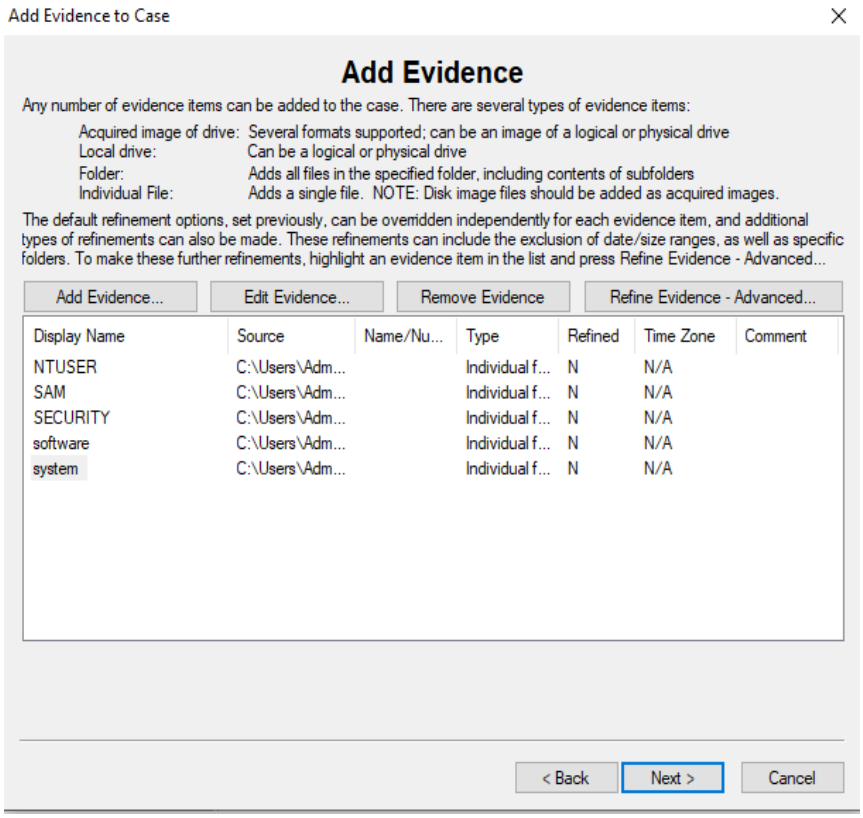


2:25 PM


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
Deletion Status:
Deleted
Not deleted
Either
Encryption Status:
Encrypted
Not encrypted
Either
Email Status:
From email
Not from email
Either
Include Duplicate Files
OLE Streams
File Type Criteria
Documents
Spreadsheets
Databases
Graphics
Multimedia
Email msgs
Executables
Archives
Folders
Other Known
Unknown
< Back
Next >
Cancel

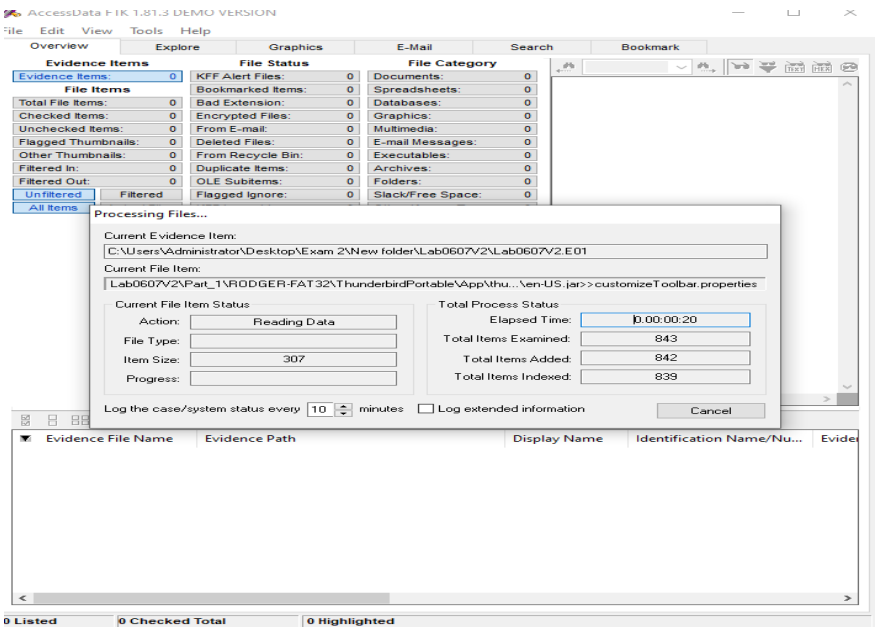

Refine Index - Default
Refine Index - Default
In order to save time and resources, and/or to make searching more efficient, you may choose to exclude certain kinds of data from being indexed. Here, you can choose default settings that will apply to each evidence item that gets added to the case. To exclude 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
Deletion Status:
Deleted
Not deleted
Either
Encryption Status:
Encrypted
Not encrypted
Either
Email Status:
From email
Not from email
Either
Include Duplicate Files
OLE Streams
File Type Criteria
Documents
Spreadsheets
Databases
Graphics
Multimedia
Email msgs
Executables
Archives
Folders
Other Known
Unknown
< Back
Next >
Cancel

2:30 PM

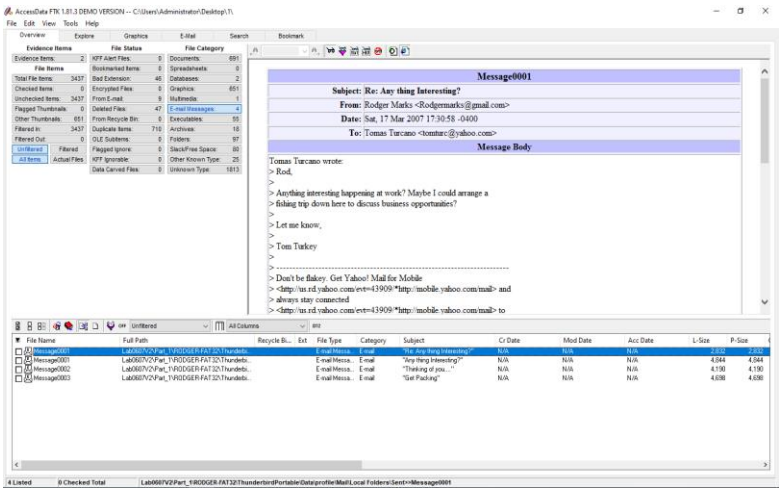


2:34 PM

Loaded the “USB drive image” on FTK.

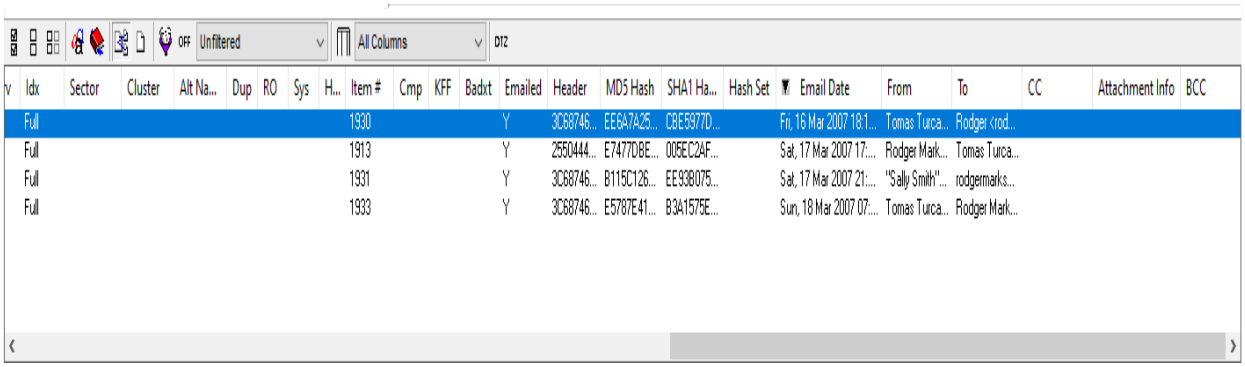


Went to the “Overview” tab of FTK and found out that there were 4 e-mails.



Sorted the emails by date

2:35 PM



Now, reading the mesaages after sorting it.

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. Get Yahoo! Mail for Mobile and
always st ay connected to friends.

Main Message Header

From - Fri Mar 16 22:46:22 2007
X-Account-Key: account2
X-UIDL: GmailId1115d78a5596d222
X-Mozilla-Status: 0003

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
> <http://us.rd.yahoo.com/evt=43909/*http://mobile.yahoo.com/mail> and
> always stay connected
> <http://us.rd.yahoo.com/evt=43909/*http://mobile.yahoo.com/mail> to
> friends.
Do you think this would be enough for a week of bonefishing?

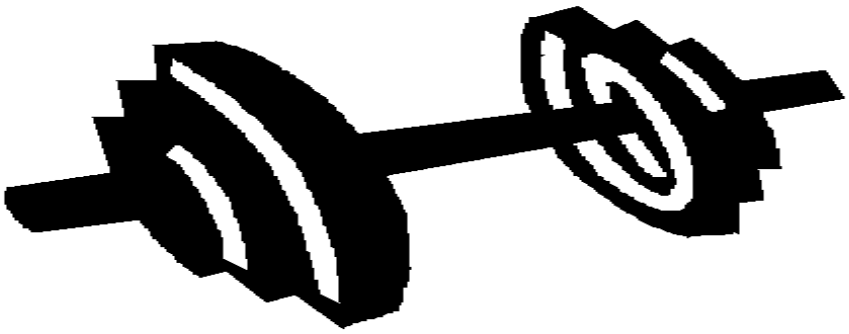
Rod

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:	rodgermarks@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

Sally

_____

i'm making a difference. Make every IM count for the cause of your choice.
Join Now.
http://clk.atdmt.com/MSN/go/msnnkwme0080000001msn/direct/01/?href=http://im.live.com/messenger/im/home/?source=hmtagline

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

CNN Money 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.

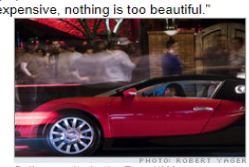


PHOTO: ROBERT VADER

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

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.

nazarian.03.jpg

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

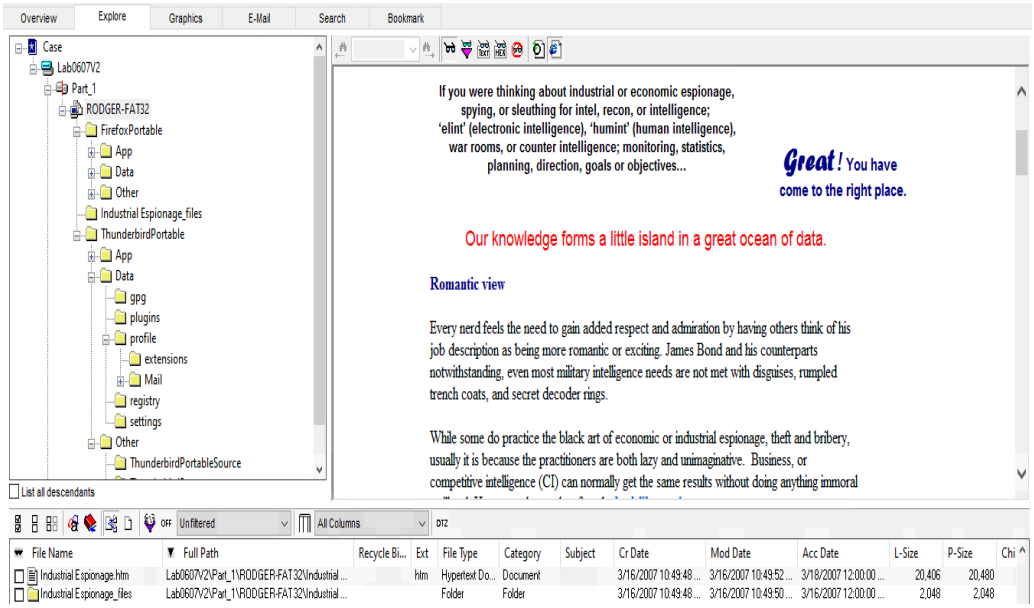
Message0003	
Subject:	Get Packing
From:	Tomas Turcano <tomturc@yahoo.com>
Date:	Sun, 18 Mar 2007 07:17:14 -0700 (PDT)
To:	Rodger Marks <rodgermarks@gmail.com>

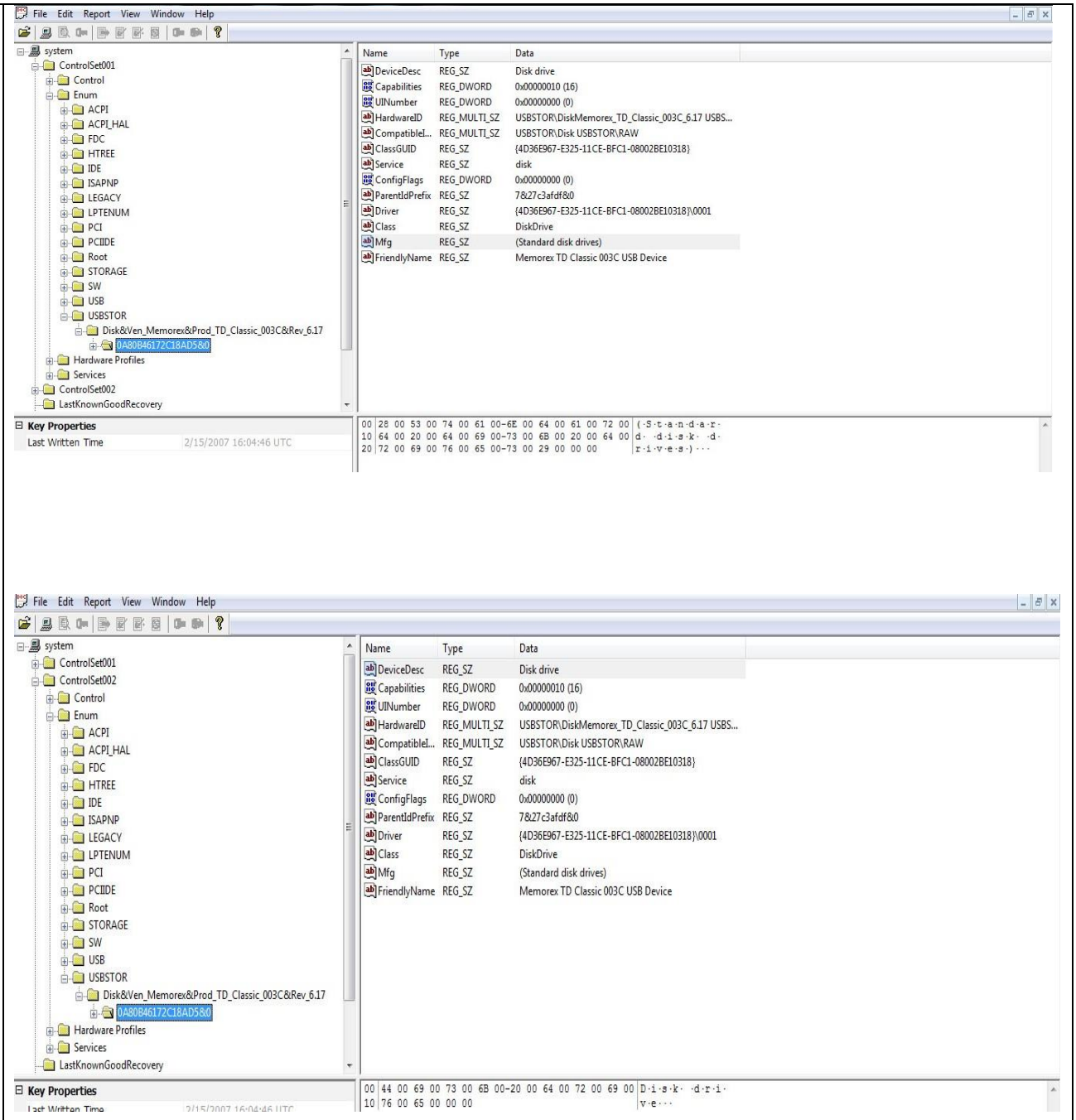
Message Body

I think you earned your fishing trip!

I'll call you at home to arrange.

Turkey

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


File Edit Report View Window Help
system
ControlSet001
Control
Enum
ACPI
ACPI_HAL
FDC
HTREE
IDE
ISAPNP
LEGACY
LPTENUM
PCI
PCIIDE
Root
STORAGE
SW
USB
USBSTOR
Disk&Ven_Memorex&Prod_TD_Classic_003C&Rev_6.17
0A80B46172C18AD58&0
Hardware Profiles
Services
ControlSet002
LastKnownGoodRecovery
Name Type Data
DeviceDesc REG_SZ Disk drive
Capabilities REG_DWORD 0x00000010 (16)
UINumber REG_DWORD 0x00000000 (0)
HardwareID REG_MULTI_SZ USBSTOR\DiskMemorex_TD_Classic_003C_6.17 USBS...
CompatibleI... REG_MULTI_SZ USBSTOR\Disk USBSTOR\RAW
ClassGUID REG_SZ {4D36E967-E325-11CE-BFC1-08002BE10318}
Service REG_SZ disk
ConfigFlags REG_DWORD 0x00000000 (0)
ParentIdPrefix REG_SZ 7&27c3afdf&0
Driver REG_SZ {4D36E967-E325-11CE-BFC1-08002BE10318}\0001
Class REG_SZ DiskDrive
Mfg REG_SZ (Standard disk drives)
FriendlyName REG_SZ Memorex TD Classic 003C USB Device
Key Properties
Last Written Time 2/15/2007 16:04:46 UTC
00 28 00 53 00 74 00 61 00-6E 00 64 00 61 00 72 00 (·S·t·a·n·d·a·r·
10 64 00 20 00 64 00 69 00-73 00 6B 00 20 00 64 00 d· ·d·i·s·k· ·d·
20 72 00 69 00 76 00 65 00-73 00 29 00 00 00 r·i·v·e·s·)···
File Edit Report View Window Help
system
ControlSet001
ControlSet002
Control
Enum
ACPI
ACPI_HAL
FDC
HTREE
IDE
ISAPNP
LEGACY
LPTENUM
PCI
PCIIDE
Root
STORAGE
SW
USB
USBSTOR
Disk&Ven_Memorex&Prod_TD_Classic_003C&Rev_6.17
0A80B46172C18AD58&0
Hardware Profiles
Services
LastKnownGoodRecovery
Name Type Data
DeviceDesc REG_SZ Disk drive
Capabilities REG_DWORD 0x00000010 (16)
UINumber REG_DWORD 0x00000000 (0)
HardwareID REG_MULTI_SZ USBSTOR\DiskMemorex_TD_Classic_003C_6.17 USBS...
CompatibleI... REG_MULTI_SZ USBSTOR\Disk USBSTOR\RAW
ClassGUID REG_SZ {4D36E967-E325-11CE-BFC1-08002BE10318}
Service REG_SZ disk
ConfigFlags REG_DWORD 0x00000000 (0)
ParentIdPrefix REG_SZ 7&27c3afdf&0
Driver REG_SZ {4D36E967-E325-11CE-BFC1-08002BE10318}\0001
Class REG_SZ DiskDrive
Mfg REG_SZ (Standard disk drives)
FriendlyName REG_SZ Memorex TD Classic 003C USB Device
Key Properties
00 44 00 69 00 73 00 6B 00-20 00 64 00 72 00 69 00 D·i·s·k· ·d·r·i·
10 76 00 65 00 00 00 v·e···