ISSA – December 4, 2015

"Computer Forensics: An Intro to Trade Secret Theft Forensics"

Presented by

Brett Creasy - CCE, CISSP, GCFA

VP & Director of Digital Forensics, bit-x-bit LLC

Example Cases

- Theft of Trade Secrets
- Workplace harassment
- Non-Compete
- Unauthorized Access (hacking)
- "Doctored" Documents

Speaking of Trade Secret Cases…

- Sales engineer of manufacturing company leaves for a direct competitor and takes design and pricing info
- Executive leaves energy company and starts a competing business, using his old employers data

Key Considerations

- ESI is Fragile
  - Easy to change
  - Easy to delete
- Once overwritten, it is gone forever
- Never work from the original evidence**
- Make a verified copy

bit-x-bit

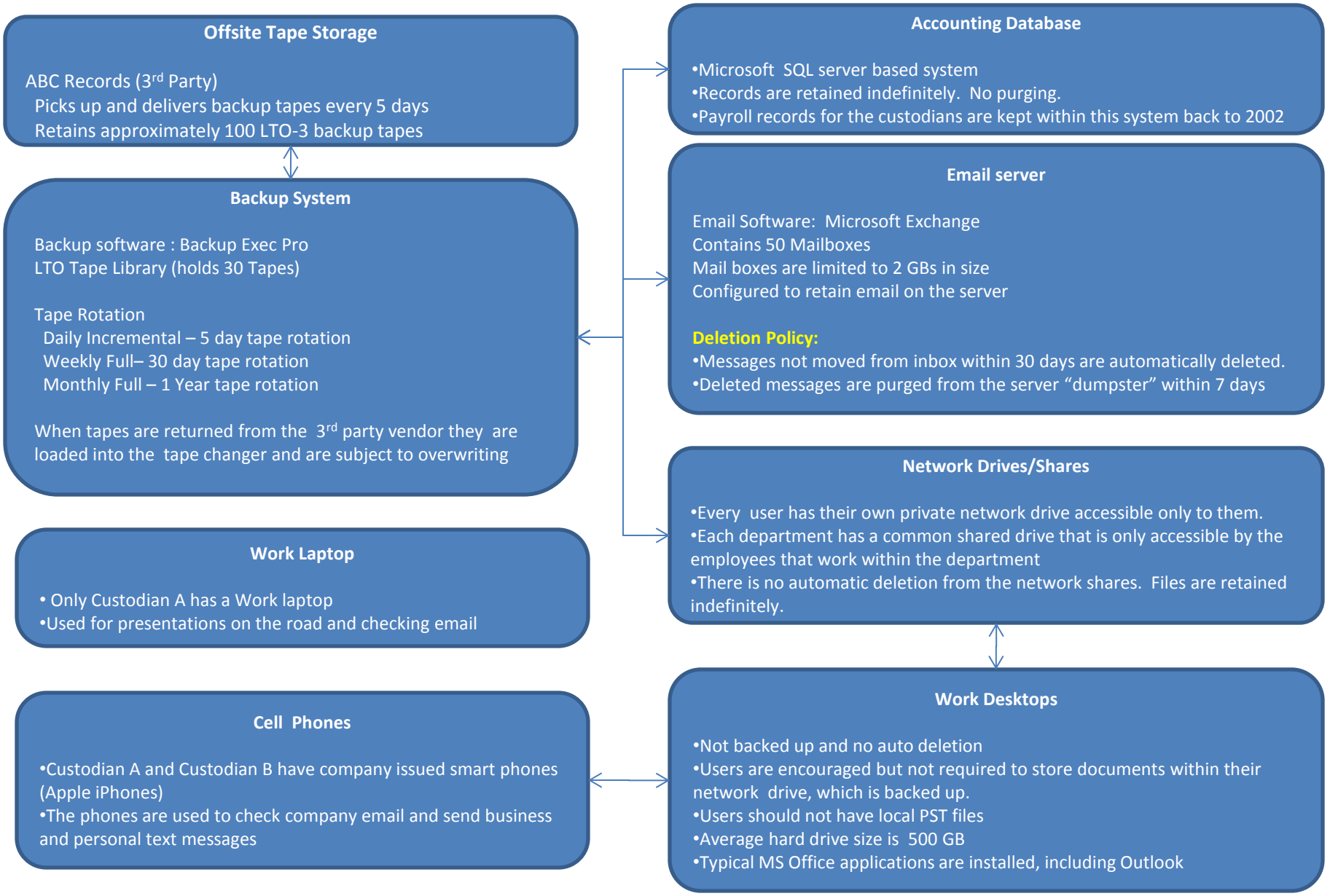
We get it.

Data Collection – Where To Go?

- Computers:
  - dead box forensic image or incident response / live
  - active email and documents (still preserve the metadata!)
- Network or End-Point Security Logs
  - SIEM < Malware, firewall, IDS/IPS, DLP, etc
- Mobile Phone:
  - Usually covers active and some deleted content
- Targeted "active" locations:
  - Email server mailbox
  - file server "shared" folder
- Social Media:
  - more than just screenshots

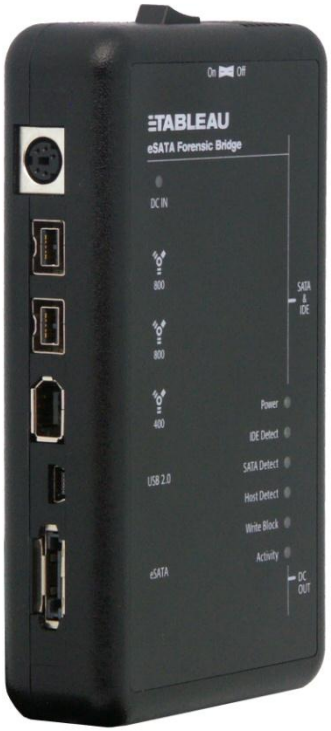
Questions to Ask

- Who are the key players and what IT systems do they use?
- Are any automated deletion processes operating on the IT Systems?
- What issues in the case will the electronic evidence need to address?
- What collection method will preserve the electronic evidence and associated metadata that will be needed to address the issues in the case?


Offsite Tape Storage
ABC Records (3rd Party)
Picks up and delivers backup tapes every 5 days
Retains approximately 100 LTO-3 backup tapes
Backup System
Backup software : Backup Exec Pro
LTO Tape Library (holds 30 Tapes)
Tape Rotation
Daily Incremental – 5 day tape rotation
Weekly Full– 30 day tape rotation
Monthly Full – 1 Year tape rotation
When tapes are returned from the 3rd party vendor they are loaded into the tape changer and are subject to overwriting
Work Laptop
• Only Custodian A has a Work laptop
•Used for presentations on the road and checking email
Cell Phones
•Custodian A and Custodian B have company issued smart phones (Apple iPhones)
•The phones are used to check company email and send business and personal text messages
Accounting Database
•Microsoft SQL server based system
•Records are retained indefinitely. No purging.
•Payroll records for the custodians are kept within this system back to 2002
Email server
Email Software: Microsoft Exchange
Contains 50 Mailboxes
Mail boxes are limited to 2 GBs in size
Configured to retain email on the server
Deletion Policy:
•Messages not moved from inbox within 30 days are automatically deleted.
•Deleted messages are purged from the server "dumpster" within 7 days
Network Drives/Shares
•Every user has their own private network drive accessible only to them.
•Each department has a common shared drive that is only accessible by the employees that work within the department
•There is no automatic deletion from the network shares. Files are retained indefinitely.
Work Desktops
•Not backed up and no auto deletion
•Users are encouraged but not required to store documents within their network drive, which is backed up.
•Users should not have local PST files
•Average hard drive size is 500 GB
•Typical MS Office applications are installed, including Outlook

Write Blocking

- Prevents inadvertent changes
- Hardware (Tableau, Wiebetech)
- Software (f-response, safe block)
- Built in media mechanisms
  (SD Cards, Floppies!)

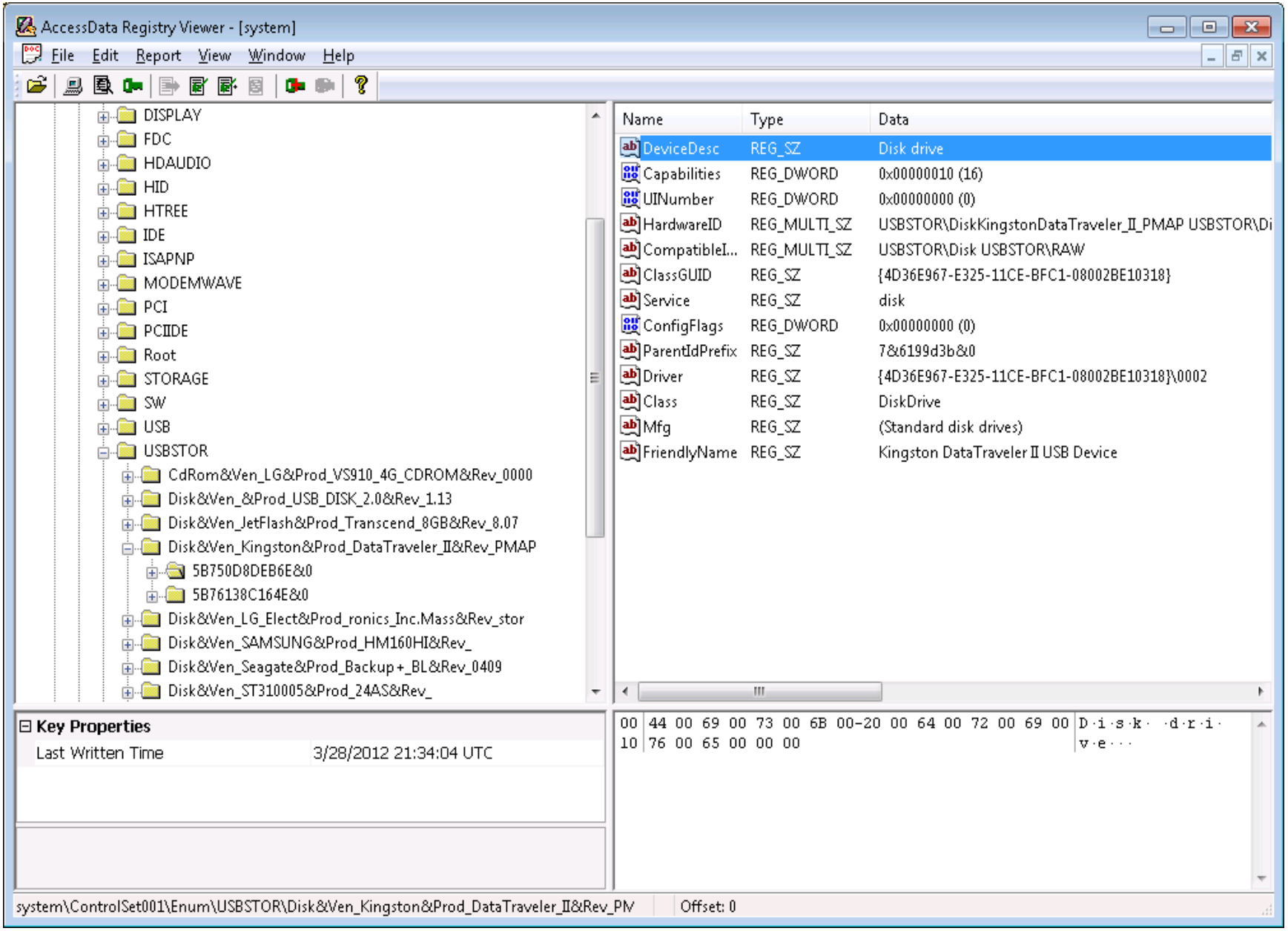


Authentication

- Chain of Custody / Record Keeping
  - photos, serial numbers, from who to who, etc
- Digital signatures (hash)
  - MD5, SHA-1

(some) Artifacts - Windows

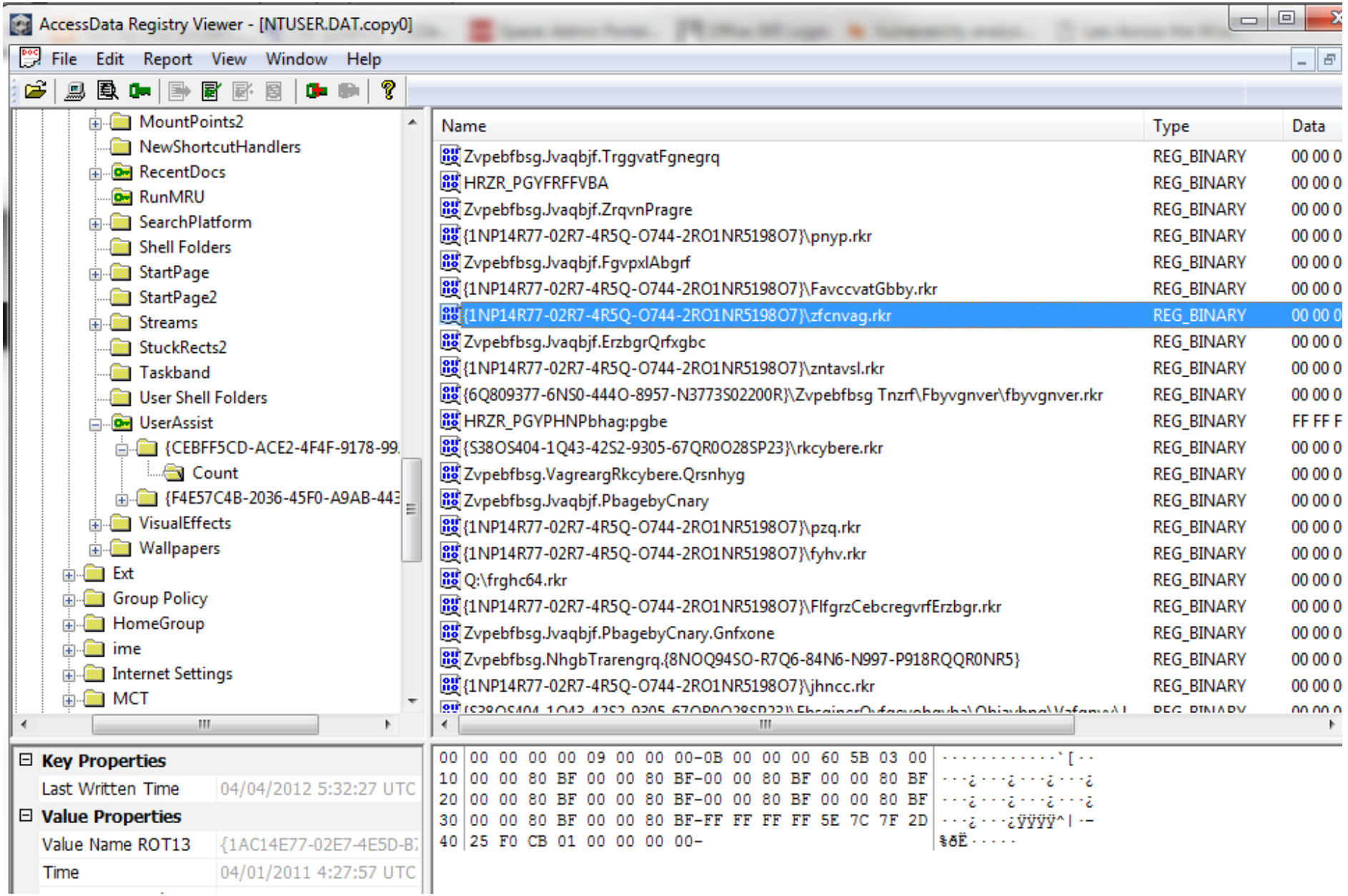
- Registry Hives
- Prefetch
- LNK files / Jumplists
- Internet Browser files
- Recycle Bin
- Filesystem
- OS Log files
- Application specific logs
- Unallocated


AccessData Registry Viewer - [system]
File Edit Report View Window Help
DISPLAY
FDC
HDAUDIO
HID
HTREE
IDE
ISAPNP
MODEMWAVE
PCI
PCIIDE
Root
STORAGE
SW
USB
USBSTOR
CdRom&Ven_LG&Prod_VS910_4G_CDROM&Rev_0000
Disk&Ven_&Prod_USB_DISK_2.0&Rev_1.13
Disk&Ven_JetFlash&Prod_Transcend_8GB&Rev_8.07
Disk&Ven_Kingston&Prod_DataTraveler_II&Rev_PMAP
5B750D8DEB6E&0
5B76138C164E&0
Disk&Ven_LG_Elect&Prod_ronics_Inc.Mass&Rev_stor
Disk&Ven_SAMSUNG&Prod_HM160HI&Rev_
Disk&Ven_Seagate&Prod_Backup+_BL&Rev_0409
Disk&Ven_ST310005&Prod_24AS&Rev_
Name Type Data
DeviceDesc REG_SZ Disk drive
Capabilities REG_DWORD 0x00000010 (16)
UINumber REG_DWORD 0x00000000 (0)
HardwareID REG_MULTI_SZ USBSTOR\DiskKingstonDataTraveler_II_PMAP USBSTOR\Di
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&6199d3b&0
Driver REG_SZ {4D36E967-E325-11CE-BFC1-08002BE10318}\0002
Class REG_SZ DiskDrive
Mfg REG_SZ (Standard disk drives)
FriendlyName REG_SZ Kingston DataTraveler II USB Device
Key Properties
Last Written Time 3/28/2012 21:34:04 UTC
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···
system\ControlSet001\Enum\USBSTOR\Disk&Ven_Kingston&Prod_DataTraveler_II&Rev_PM
Offset: 0

Registry USB Deliverable

Device	Serial Number	First Recognized	Last Recognized
BUFFALO HD-PXU2 USB Device	0010100703057X370	10/12/2011 08:50:11 AM	10/31/2013 11:34:33 AM
USB Flash Disk USB Device	CCBB02010101490867531	12/17/2011 10:39:21 AM	10/15/2013 09:46:42 AM
USB 2.0 USB Flash Drive USB Device	AA0000000358791	05/06/2013 03:25:28 PM	05/07/2013 09:52:16 AM
Kindle Internal Storage USB Device	B00E150115230ST	12/20/2011 09:51:16 AM	05/01/2013 06:22:01 AM
Flash Drive AU_USB2.0 USB Device	SI7J9II7	01/23/2012 03:14:11 PM	01/29/2013 05:14:19 PM
SanDisk Cruzer Mini USB Device	2004101610cf0d3227c	12/14/2012 02:19:36 PM	12/21/2012 03:19:39 PM
USB Flash Disk USB Device	CCBC131101303319775009	08/08/2012 03:46:01 PM	08/15/2012 05:46:03 PM
USB 2.0 Flash disk USB Device	1000000DB7893	02/15/2011 10:22:49 AM	02/14/2012 09:22:52 PM
USB2.0 Flash Disk USB Device	f150f7c	10/13/2011 11:55:53 AM	10/21/2011 12:31:30 PM
SanDisk Cruzer Blade USB Device	2004431743031FB13BA	06/16/2011 02:19:45 PM	08/15/2011 07:59:21 AM
SanDisk Cruzer Blade USB Device	2004432280087FB83FC0	06/01/2011 10:44:46 AM	06/01/2011 10:44:48 AM
hp v125w USB Device	AA0C100209935636	05/12/2011 04:08:01 PM	05/19/2011 02:52:07 PM

Registry – Need to Unscramble Things First!



Registry – User Assist

```
Tue Jan  7 13:56:56 2014 Z
  {6D809377-6AF0-444B-8957-A3773F02200E}\CCleaner\CCleaner64.exe (17)
Thu Jan  2 20:08:44 2014 Z
  {6D809377-6AF0-444B-8957-A3773F02200E}\SUPERAntiSpyware\SUPERAntiSpyware.exe (2)
Thu Jan  2 12:48:16 2014 Z
  {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Petro Vend\Phoenix\P4W.exe (1)
Tue Dec 31 16:13:28 2013 Z
  {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Malwarebytes' Anti-Malware\mbam.exe (1)
Mon Dec 30 16:12:36 2013 Z
  C:\Users\jdoe\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\YTC2D3NN\ccsetup409.exe (1)
```

Prefetch

- **Naming convention…**
  cmd.exe-06264562.pf
- **What does a prefetch file tell us?**
  - **Name** of the executable (or software application)
  - List of **DLL files** used by that software
  - **Count** of how many times the software program has been run
  - **Timestamp** identifying the last time the program was run

- Antiforensic tools
  - Wiping tools
  - Time modification tools
- Software installed on a system
  - Uncommon cloud applications
- Malicious activity
  - File paths with users not authorized to use the system

Recycle Bin (Win 7+)

- $I files contain the info regarding what was deleted (original name, path, deletion date/time, size)
- $R files are the actual deleted files

$II3DF3L.zip
$IUUH4BS.library-ms
$R3TPCIK.library-ms
$R3TPCIK.library-ms.Fil...
$R6MHA5W
$R8XLAY7
$RI3DF3L.zip
$RUUH4BS.library-ms
$RUUH4BS.library-ms.Fi...

LNK Files

Link target information	
Local Path	G:\Quotes\CustomerX\CustomerX.pdf
Volume Type	Removable Disk
Volume Serial Number	DA74-E37F
File size	307749
Creation time (UTC)	9/6/2007 5:09:40 PM
Last write time (UTC)	7/18/2007 2:23:14 PM
Last access time (UTC)	3/23/2008 4:00:00 AM

LNK Files

Full Path	Created Date	Modified Date	Accessed Date
\Part_2\NONAME-NTFS\Documents and Settings\JSmith\Recent\CustomerX.lnk	3/23/2008 11:09	3/23/2008 11:09	3/23/2008 11:09

Unallocated

Sounds good, talk then.
 Sam

 On Thu, Nov 22, 2013 at 8:03 AM, Jim Smith <jimsmithfakeemail@gmail.com>

wrote:
blockquote class="gmail_quote" style="margin:0 0 0 .8ex;border-left:1px #ccc solid;padding-left:1ex"> Sam, lets talk at 10:30am heading into a meeting.
 Chat soon

 Regards, Jim Jim Smith Vice President of HR Your Biggest Competitor Inc 555-867-5309 mobile
On Nov 22, 2013, at 7:27 AM, Sam Smith <samsmithfakeemail@gmail.com> wrote:

 <blockquote type="cite"> Jim,
 Sorry I couldnt call last night.
 Does 8 AM work on your end?
 Thanks,
 Sam

Unallocated

Sounds good, talk then.
 Sam

 On Thu, Nov 22, 2013 at 8:03 AM, Jim Smith <jimsmithfakeemail@gmail.com>
wrote:
blockquote class="gmail_quote" style="margin:0 0 0 .8ex;border-left:1px #ccc solid;padding-left:1ex"> Sam, lets talk at 10:30am heading into a meeting.

 Chat soon

 Regards, Jim
Jim Smith Vice President of HR Your Biggest Competitor Inc
555-867-5309 mobile
On Nov 22, 2013, at 7:27 AM, Sam Smith <samsmithfakeemail@gmail.com>
wrote:

 <blockquote type="cite"> Jim,
 Sorry I couldnt call last night.
 Does 8 AM work on your end?
 Thanks,
 Sam

Unallocated

Sounds good, talk then.

Sam

On Thu, Nov 22, 2013 at 8:03 AM, Jim Smith <jimsmithfakeemail@gmail.com> wrote:

> Sam, lets talk at 10:30am heading into a meeting.
>
> Chat soon
>
> Regards,
> Jim
> Jim Smith
> Vice President of HR
> Your Biggest Competitor Inc
> 555-867-5309 mobile
>
> On Nov 22, 2013, at 7:27 AM, Sam Smith <samsmithfakeemail@gmail.com> wrote:
>
> > Jim,
> >
> > Sorry I couldnt call last night.
> >
> > Does 8 AM work on your end?
> >
> > Thanks,
> >
> > Sam

Why Memory?

- Correlate or expand on findings from disk and log analysis
- Find things not present on disk (malware)
- Everything from the OS goes through RAM
- Network connections, IP addresses, URLs
- Encryption keys/passwords

Memory – How To Get It

- Capture it live (memory dump)
  - Moonsols (DumpIt)
  - Volatility
  - Memoryze
  - Redline
- Hibernation File (hiberfil.sys from your disk analysis)
- Virtual Machines
  - .vmem (Vmware)
  - .mem (Parallels)
  - .bin (MS Hyper-V)

Questions

Brett Creasy - CCE, CISSP, GCFA
VP & Director of Digital Forensics
brett.creasy@bit-x-bit.com

bit-x-bit, LLC
Frick Building
Pittsburgh, Pennsylvania