



Computer Forensics

Mr. Raghu Kumar L

Overview

- Introduction
- What happens when a file is deleted
- Typical Computer Forensic Investigations
- Who uses Computer Forensics
- Important things to remember
- Options to avoid
- Computer Forensic software
- EnCase Forensic
- How to become a Computer Forensic Examiner
- Conclusion

What is Computer Forensics?

- Collection, preservation, analysis and presentation of computer-related evidence
- Determining the past actions that have taken place on a computer system using computer forensic techniques

What is the Purpose of Computer Forensics?

- Classic Forensics
- Computer forensics uses technology to search for digital evidence of a crime
- Attempts to retrieve information even if it has been altered or erased so it can be used in the pursuit of an attacker or a criminal
- Incident Response
 - Live System Analysis
- Computer Forensics
 - Post-Mortem Analysis

What Happens when a File is Deleted?

- Windows Operating System
 - File Allocation Table (FAT)
 - Master File Table (MFT)
- FAT/MFT tells the computer where the file begins and ends
- Deleted pointers to the file
 - FAT/MFT space occupied by the file is mark as available
- The actual data that was contained in the file is not deleted
 - Unallocated space

Typical Investigations

- Theft of Company Secrets (client, customer or employee lists)
- Employee Sabotage
- Credit Card Fraud
- Financial Crimes
- Embezzlement (money or information)
- Economic Crimes
- Harassment
- Child Pornography
- Major Crimes
- Identity Theft

Media Devices that hold Potential Data

- Computers and laptops
- iPads
- iPods
- Smartphones and most other cell phones
- MP3 music players
- Hard Drives
- Digital Cameras
- USB Memory Devices
- PDAs (Personal Digital Assistants)
- Backup Tapes
- CD-ROMs & DVD's

Computer Forensic Capabilities

- Recover deleted files
- Find out what external devices have been attached and what users accessed them
- Determine what programs ran
- Recover webpages
- Recover emails and users who read them
- Recover chat logs
- Determine file servers used
- Discover document's hidden history
- Recover phone records and SMS text messages from mobile devices
- Find malware and data collected

Who uses Computer Forensics?

- Law Enforcement
- Private Computer Forensic Organizations
- Military
- University Programs
- Computer Security and IT Professionals

Law Enforcement

- Local, State and Federal levels
- Several detectives at local levels
 - **Inadequate funding**
- State Police
- FBI's Computer Analysis and Response Team (CART)
- Regional Computer Forensics Laboratories (RCFLs)
 - **Philadelphia**
- Primarily use EnCase

Private Computer Forensic Organizations

- Radley Forensics
- Computer Forensics Associates
- Bit-X-Bit
- Empire Investigation LLC
- Marmo Technology
- Advanced Forensic Recovery of Electronic Data
- Philadelphia Computer Forensics
- Philadelphia Computer Forensics Analysis and Investigations
- New York Computer Forensic Services
- Speckin Forensic Laboratories

Military

- Test, identify, and gather evidence in the field
 - Specialized training in imaging and identifying multiple sources of electronic evidence
- Analyze the evidence for rapid intelligence gathering and responding to security breach incidents
 - Desktop and server forensic techniques

University Programs

- Bachelors and Masters degrees
 - Incident response techniques
 - Well funded research area
 - Many free sources of test images to practice on
- Community colleges
 - Partnering with 4-year universities to complete associates and bachelors degrees
 - Great for working professionals
 - Flexible schedules and affordable tuition

Computer Security Professionals and IT Personnel

- Network traffic
- Compromised networks
- Insider threats
 - Disloyal employees
- Malware
- Breach of contracts
- E-mail Fraud/Spam
- Theft of company documents

Important Factors

- Legal procedures
 - **Not compromising evidence**
- Treat every piece of evidence as it will be used in court
- Documentation*
- Chain of Custody
- Write Blocks
- Imaging
 - **Bit by bit copy of a piece of electronic media (Hard drive)**

What Should be Avoided During an Investigation?

- Changing data
 - Changing time or date stamps
 - Changing files
- Overwriting unallocated disk space
 - This can happen when re-booting
- Verify Hash values from images

Computer Forensic Tools

- Parse through the created image
 - **Built in system parser**
- Rebuilds both active and deleted files
- Open source
- Commercial sources

Common Computer Forensic Software

- ArcSight Logger
- Netwitness Investigator
- Quest Change Auditor
- Cellebrite
- Physical Analyzer
- Lantern
- Access Data's Forensic Toolkit (FTK)
- EnCase Cybersecurity
- EnCase eDiscovery
- EnCase Portable
- EnCase Forensic*

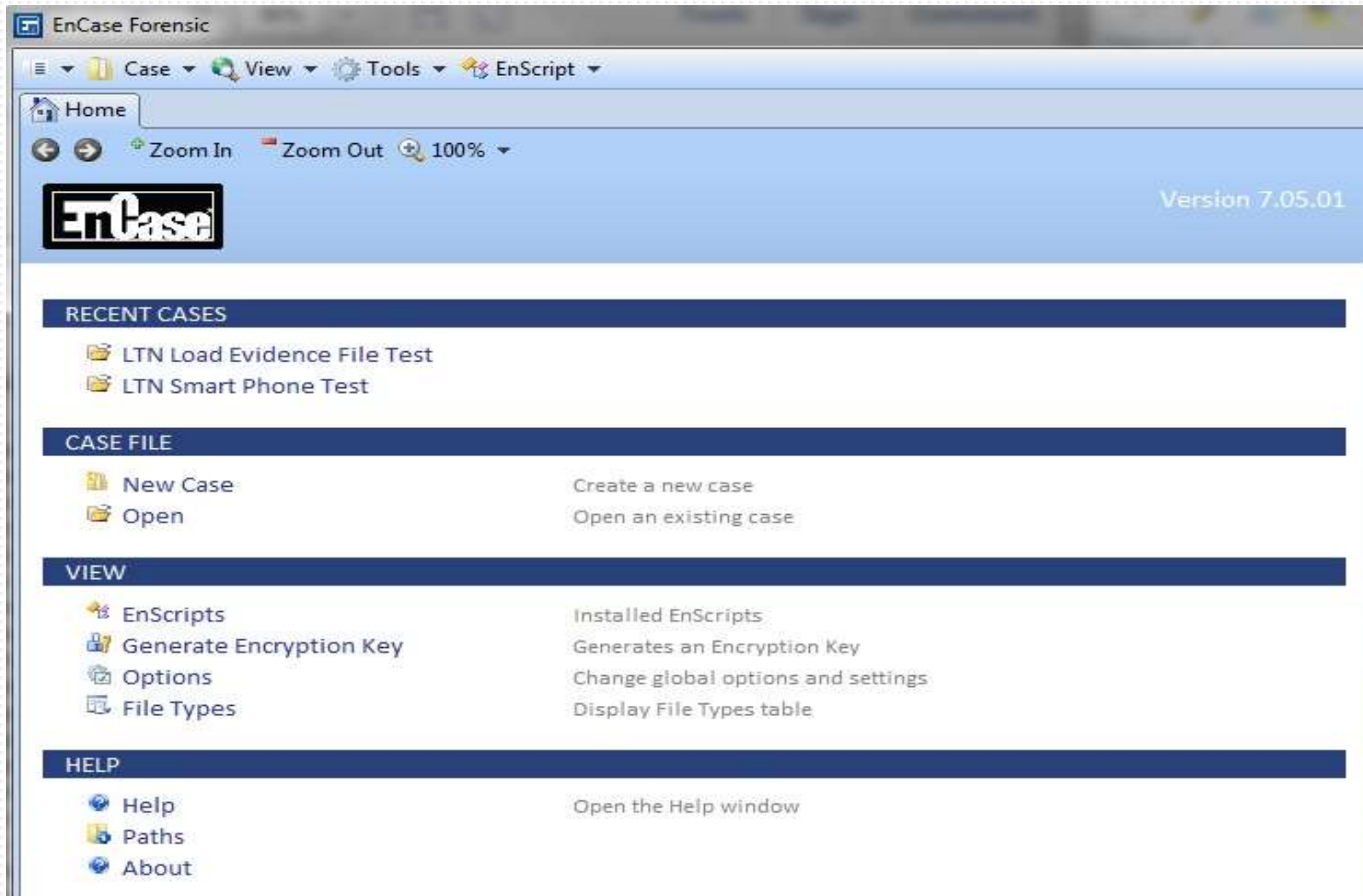
EnCase Forensic

- Acquisition
- Reporting
- EnScript :
 - Scripting facility
 - Various API's for interacting with evidence
- Collect, Analyze and examine data
 - Deleted files
 - Unallocated space
 - File slack
- Duplicates of original data (Imaging)
 - Accuracy can be verified by hash and Cyclic Redundancy Check values

EnCase Forensic

- Many operating systems
 - Windows
 - Linux
 - Apple iOS
 - Sun/Oracle Solaris
- Supported smartphones
- Recommended to run on Window 7 (64 bit) operating system

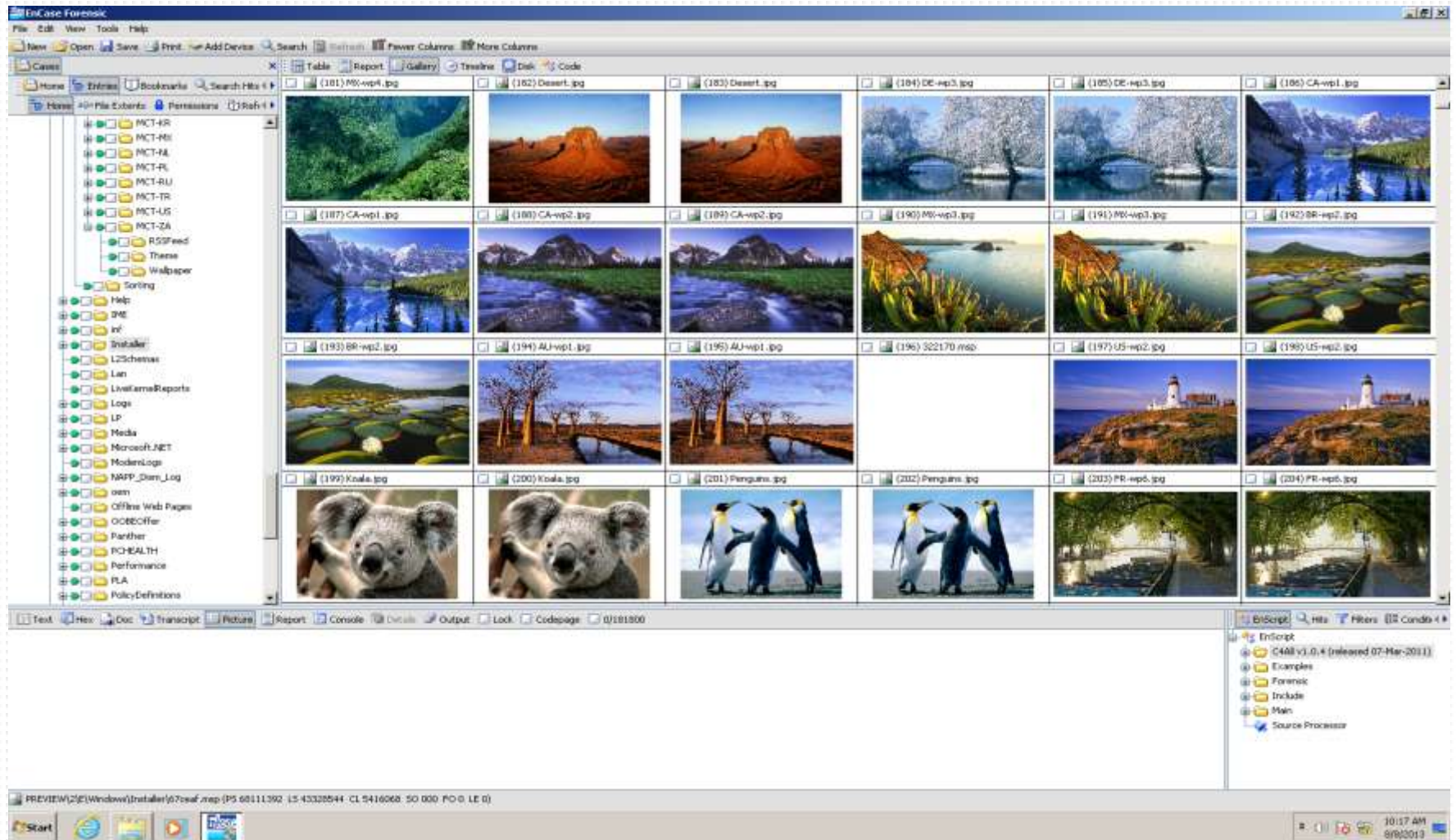
EnCase Forensic



File Signatures

File Signatures				
<div> <div>Add</div> <div>Edit</div> <div>Delete</div> <div>Export</div> <div>Import</div> <div>Close</div> </div>				
	Ext	Alias	Category	Viewer
<input type="checkbox"/> 1	exe	EXE File	Executable	EnCase
<input type="checkbox"/> 2	com	COM File	Executable	EnCase
<input type="checkbox"/> 3	bat	Batch File	Executable	EnCase
<input type="checkbox"/> 4	dll	Dynamic Link Library	Library	EnCase
<input type="checkbox"/> 5	class	Java Class Library	Library	EnCase
<input type="checkbox"/> 6	reg	Registry File	Registry	EnCase
<input type="checkbox"/> 7	wav	Waveform Audio File	Sound	Windows Default
<input type="checkbox"/> 8	avi	Video File	Movie	Windows Default
<input type="checkbox"/> 9	ttf	True Type Font	Font	EnCase
<input type="checkbox"/> 10	rtf	Rich Text Format	Document	Windows Default
<input type="checkbox"/> 11	bmp	Bitmap Image	Picture	Windows Default
<input type="checkbox"/> 12	dib	Bitmap	Picture	Windows Default
<input type="checkbox"/> 13	gif	GIF	Picture	Windows Default
<input type="checkbox"/> 14	jpg	JPEG	Picture	Windows Default
<input type="checkbox"/> 15	html	Web Page	Document	Windows Default

EnCase Gallery





EnCase Document View

The screenshot shows the EnCase Forensic software interface. The main window displays a list of files with columns for Name, Filter, In Report, File Ext, File Type, File Category, Signature, Description, and Is Deleted. The left pane shows a tree view of the file system. The bottom pane shows a list of actions related to the selected file.

Name	Filter	In Report	File Ext	File Type	File Category	Signature	Description	Is Deleted
21		NO	.xml	XML Document	Document		File, Archive, Hard Linked	NO
22		NO	.xml	XML Document	Document		File, Archive	NO
23		NO	.xml	XML Document	Document		File, Archive, Hard Linked	NO
24		NO	.xml	XML Document	Document		File, Archive, Hard Linked	NO
25		NO	.xml	XML Document	Document		File, Archive, Hard Linked	NO
26		NO	.xml	XML Document	Document		File, Archive, Hard Linked	NO
27		NO	.xml	XML Document	Document		File, Archive	NO
28		NO	.xml	XML Document	Document		File, Archive, Hard Linked	NO
29		NO	.xml	XML Document	Document		File, Archive, Hard Linked	NO
30		NO	.xml	XML Document	Document		File, Archive, Hard Linked	NO
31		NO	.xml	XML Document	Document		File, Archive	NO
32		NO	.xml	XML Document	Document		File, Archive, Hard Linked	NO
33		NO	.xml	XML Document	Document		File, Archive, Hard Linked	NO
34		NO	.xml	XML Document	Document		File, Archive, Hard Linked	NO
35		NO	.xml	XML Document	Document		File, Archive	NO
36		NO	.xml	XML Document	Document		File, Archive, Hard Linked	NO
37		NO	.xml	XML Document	Document		File, Archive	NO
38		NO	.xml	XML Document	Document		File, Archive, Hard Linked	NO

Wireless Network Troubleshooter

Insert Wireless Network Troubleshooting Tables

Create Registry Wireless Adapter Table

Create Wireless Network Connection Attempts Table

Create Network Wireless Summary Table

Check For Enabled Wireless Adapters

Check For Wireless Auto-Configuration Service

Stopped

Check Wireless Network Connection Attempts

Summarize Network Wireless Summary Table

Wireless Network Cleanup

Insert Information List

PREVIEW(D:\Windows\PAI\Rules\en-US\Rules\System.Wireless.xml (PS 46354480 LS 21571632 CL 2690454 SO 000 PO 0 LE 0))

Perform a Search

- Raw Search
 - A search based on keywords that search the entire drive for a match
 - Slow process on larger drives
- Indexed Search
 - A search that requires the drive to be indexed
 - Indexing can take a long time
 - Searches are instantaneous

Bookmark Specific Evidence

- Bookmark Findings
 - Raw Text Bookmarks
 - Data Structure Bookmarks
 - Notable File Bookmarks
 - Multiple Notable File Bookmarks
 - Note Bookmarks
 - Table Bookmarks
 - Transcript Bookmarks

Indexed Search

EnCase Forensic

Case (LTN Load Evidence File Test) View Tools EnScript Add Evidence

Home Evidence Search

Viewing (Search) Split Mode Condition Filter Searches Tags Review Package Raw Search Results Bookmark Go to file

Index

Tyler and Business

	Word	Hits	Items
1	business	1,615	372
2	business'	4	3
3	business.com	2	1
4	business2telephonenu...	1	1
5	business_and_economy	2	2
6	business_and_shopping	4	2
7	business_at_hand_idiom	1	1
8	business_credit_cards	6	4
9	business_exchange	1	1
10	business_finance	2	2
11	business	1	1

	Name	Tag	File Ext	Logical Size	Item Type	Category	Si A
64	animator[1].js		js	13,562	Document	Script	Matc
65	rss[1].xml		xml	15,825	Document	Document	Matc
66	download[1].htm		htm	18,920	Document	Document	Matc
67	footer[1].htm		htm	25,041	Document	Document	Matc
68	google_com[1].htm		htm	26,642	Document	Document	Matc
69	hiding_text_in_text_steganography_project[1].htm		htm	27,967	Document	Document	Matc
70	110317-224244_adv_11[1].htm		htm	28,605	Document	Document	Matc
71	search[1].htm		htm	32,203	Document	Document	Matc
72	2B08EC33d01			33,185	Document	Document	Alias
73	flashplayer[1].htm		htm	36,903	Document	Document	Matc
74	_CACHE_003_			40,202	Document	Document	Alias
75	google_com[1].htm		htm	41,101	Document	Document	Matc
76	_CACHE_003_			57,135	Document	Document	Alias

Fields Report Text Hex Decode Doc Transcript Picture Review Console

Find Find Next Compressed View Previous Item Next Item Fit To Page

30 • /directory/Business
33 Business
70 • /Directory/Business
71 Business
377 Everybody has a right to privacy and business secrets. You have a little
381 life or business) from unauthorized viewers. Free download of ViewPoint 5.01,

LTN Load Evidence File Test\Internet\Internet Explorer (Windows)\Cache\HTML\hiding_text_in_text_steganography_project[1].htm (TO 0 LE 0)

Bookmark Screen

EnCase Forensic Training

Case (Lab 3) View Tools EnScript Add Evidence

Home Evidence Search Bookmarks

Viewing (Bookmark) Split Mode Tags Edit Add Note Delete Folder Bookmark Go to File Find Related

Bookmarks

	Name	Comment	Tag	File Ext	Logical Size	Item Type	Category
<input type="checkbox"/> 1	Documents	The below bookmark...				0 None	
<input type="checkbox"/> 2	Pictures					0 None	
<input type="checkbox"/> 3	Email	The below bookmark...				0 None	
<input type="checkbox"/> 4	Internet Artifacts	The below bookmark...				0 None	
<input type="checkbox"/> 5	Literature	Collection of literature				0 None	

Table Timeline Gallery

Selected 0/13 Edit Add Note Delete Folder

Fields Report Text Hex Decode Doc Transcript Picture Lock

Name	Value
Name	Documents
Comment	The below bookmarks represent documents that are potentially relevant to this case.
Tag	
File Ext	

Lab 3\Documents

Start EnCase Forensic Train... Bretz_Kelsey.docx - Micr...

4:01 PM

Deleted Files

<input type="checkbox"/>	8	exFAT.E01	05/25/10 01:15:30PM	05/25/10 01:16:00PM	05/25/10 01:16:00PM
<input type="checkbox"/>	9	exFAT (Extended FAT)-Hamm-5-26-201...	03/27/10 12:26:26PM	05/25/10 01:09:18PM	05/25/10 01:09:18PM
<input type="checkbox"/>	10	ReadyBoostPerfTest.tmp	06/25/10 10:00:16AM	06/25/10 10:00:14AM	06/25/10 10:00:16AM
<input type="checkbox"/>	11	EDT (UTC-4hrs).txt	06/25/10 10:00:24AM	06/25/10 10:00:24AM	06/25/10 10:00:24AM
<input type="checkbox"/>	12	Deleted.txt	05/25/10 01:09:56PM	05/25/10 01:09:42PM	05/25/10 01:09:56PM
<input type="checkbox"/>	13	UTC.txt	06/25/10 03:00:58PM	06/25/10 03:00:58PM	06/25/10 03:00:58PM
<input type="checkbox"/>	14	Berlin (UTC+1hr).txt	06/25/10 04:01:40PM	06/25/10 04:01:40PM	06/25/10 04:01:40PM
<input type="checkbox"/>	15	Kathmandu (UTC+5.45hr).txt	06/25/10 07:47:20PM	06/25/10 07:47:20PM	06/25/10 07:47:20PM
<input type="checkbox"/>	16	EDT (UTC-4hrs).txt	06/25/10 10:04:32AM	06/25/10 10:04:32AM	06/25/10 10:04:32AM
<input type="checkbox"/>	17	New Text Document.txt	06/25/10 02:05:32PM	06/25/10 02:05:32PM	06/25/10 02:05:32PM
<input type="checkbox"/>	18	UTC.txt	06/25/10 02:05:32PM	06/25/10 02:05:32PM	06/25/10 02:05:32PM
<input type="checkbox"/>	19	Berlin Time (UTC+1hr).txt	06/25/10 04:06:12PM	06/25/10 04:06:12PM	06/25/10 04:06:12PM
<input type="checkbox"/>	20	Kathmandu (UTC+5.45hr).txt	06/25/10 07:51:58PM	06/25/10 07:51:58PM	06/25/10 07:51:58PM
<input type="checkbox"/>	21	BobbyHelmsLyrics.txt	05/25/10 01:07:56PM	05/25/10 01:08:56PM	05/25/10 01:08:56PM
<input type="checkbox"/>	22	New Text Document.txt	06/25/10 03:00:58PM	06/25/10 03:00:58PM	06/25/10 03:00:58PM

EIC2010 (F:)



Search CEIC2010

Burn New folder

Name	Date modified	Type	Size
 Berlin Time (UTC+1hr).txt	6/25/2010 10:06 AM	Text Document	0 KB
 EDT (UTC-4hrs).txt	6/25/2010 10:04 AM	Text Document	0 KB
 Kathmandu (UTC+5.45hr).txt	6/25/2010 10:07 AM	Text Document	0 KB
 UTC.txt	6/25/2010 10:05 AM	Text Document	0 KB

How to get Started

- Step 1: Obtain a degree
 - Today a bachelors degree is favored
 - FBI prefers a different scholarly degree over computer forensics
- Step 2: Get Certified
 - EnCase Certified Examiner (EnCE)
 - Computer Forensics Examiner (CCFE)
 - Certified Computer Examiner (CCE)
 - Some states require a Private Investigator License
- Step 3: Find a Job
 - Law Enforcement (Local, State, Federal)
 - Homeland Security offices, the NSA and the FBI have a growing need for examiners
 - Military
 - Private Firms
 - IT/Security Professions

<http://www.youtube.com/watch?v=vJdME6vczeo>

Conclusion

- Computer Forensics helps determine the WHO, WHAT, WHEN, and WHERE related to a computer-based crime or violation.
- Who uses Computer Forensics
- Situations to use Computer Forensics
- Computer Forensic Software
- Do and Don'ts of practicing Computer Forensics
- How to get involved in Computer Forensics

References

- <http://www.computer-forensics.net/>
- <http://www.scmagazine.com/best-computer-forensics-tool/article/195999/>
- http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202584495563&Product_Review_Encase_Forensic_7&slreturn=20130405160529
- <https://www.ncjrs.gov/pdffiles1/nij/183451.pdf>
- <http://www.westwood.edu/programs/school-of-technology/computer-forensics-online-degree/law-enforcement-computer-forensics>
- Computer Forensics: Info Sec Pro Guide
- Security Guide to Network Security Fundamentals

Questions?