



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-RÔMs & 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

KG REDDY College of Engineering

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





File Signatures

Ad	d Edit	Edit Delete I		Import	Close	
	Ext	Alias	3	Category	Viewer	
1	exe	EXE File	E	xecutable	EnCase	
2	com COM File		E	xecutable	EnCase	
3	bat Batch File		E	xecutable	EnCase	
4	dll Dynamic Link Library		Library Li	ibrary	EnCase	
5	class	Java Class L	ibrary Li	ibrary	EnCase	
6	reg	Registry File	R	egistry	EnCase	
7	wav	Waveform A	udio File S	ound	Windows Default	
8	avi	Video File	M	lovie	Windows Default	
9	ttf	True Type Fo	ont F	ont	EnCase	
10	rtf	Rich Text For	rmat D	ocument	Windows Default	
11	bmp	Bitmap Image	Pi	icture	Windows Default	
12	dib	Bitmap	Pi	icture	Windows Default	
13	gif GIF		Pi	icture	Windows Default	
14	ipg JPEG		Pi	icture	Windows Default	
15	html	Web Page	D	ocument	Windows Default	



ļ

EnCase Gallery

Canat	X Table Report Galary					
Hone Stifree UBcoknaris C.Search ?	the 6 + 🛄 (181) MX-wp4.jpg	(162) Desert.jpg	(183) Desert.pg	(104) DE-eq:3, (pg	Ci iii (185) DE-Hp3.5pg	(106) CA-wp1.jpg
🖸 Have 🕬 Pia Exteriz 🔒 Pernansara 🗍 P	alid •	1		alle de la serie	A share the second	and the second second
INCT-KR			-	and the set of the		All State Shirts
H DI CO MCT-MI		and the second se	and the second se			and the second
III OCI CO MCT-FAL			and the second se	A CONTRACTOR OF A		
B D C C FK			and the second second	and the second division of the local divisio	and the second second	State of the second second
H MCT-TR				CONTRACTOR OF A	and the second states of the s	
IN CT-US	1117) CA-wp1.3pg	CI CI (100) CA-wp2.tpg	(109) CA-wp2.pg	Eq. Cov-3M (DPL)	191) MX-wp3.10g	(192) 8R-Hp2, pg
u 🖝 🔂 🔛 MCT-ZA						and the second se
P RSSFeed	A STATISTICS	Alle Andrea	Alle allera		die die	
Diana Theres	and a state of the state	State of the second	WAR STATE OF USA ST	AND TRACK	THE REAL PROPERTY OF	And the second of the low to second
- Sorting		article	and the second s	A SAME DE LA		A A A A A A A A A A A A A A A A A A A
iii 🖝 🖂 📥 Help	ALC: NOT A			N8 1370	NK 19762	1000
1942 C C C C C C C C C C C C C C C C C C C		The second second second	Contract States			
	N			Excelence of the second		
Distaler Distaler Distaler Distaler	(193) 88-wp2, pg	[] 🔄 (194) AU-wptjbg	(195) AU-wp1.jpp	🗔 🖼 (196) \$22170 msp.	(197):05-wp2.gog	(198) US-wp2, pg
- Lan		Salar .				
DiveterneReports	No. of Concession, Name	- The second second		and the second se	1	and a second sec
a 🕒 🔁 Logs	and the second second		A A A A A A A A A A A A A A A A A A A		and the second second	
IP CIC	A DE COM					
B D C Necks			State of the Party	a table	Contraction of the second	and the second second
- ModersLogs						
B . NAFP_Darn_Log	I I I III (199) Knale tog	(1 (200) Koala (pg	(201) Pangumu pg	(202) Pengama ang	(203) PR-ep6. pg	(204) PR-ept. jpg
a la com				The second second second		
Ciffine Wids Pages	12.0				Chowles - Chippen	The state of the second
Other					CARD CONTRACTOR	
BONEALTH	Contraction of the				A WARD AND A STATE	
B Porformance	A CARLON A	A REAL PROPERTY AND			and the second s	
BOC RA	CA CONTRACTOR	A SSA				
PolicyDefinitions						Constant and the second s
ext 💭 Hex 🔔 Doc 🐏 Transcript 🛄 Pietur	🗑 🔄 Report 🛄 Console 🕲 Details 🥔 G	Dutput 🖾 Lock 🖾 Codepage 🖾 (Q1815	900			BiScript Q His T Hers (III Conde
						al es InScript
						🛊 😂 C4AB v3.0.4 (released 07-Mar-2011
						(a) 🛄 Ecomplete
						🗰 🧰 Forensic
						a California
						Source Processor
						THE SOLD FRANCE

listari 🥥 🧾 💽 🧱

* ()) 10 57 AM



a

EnCase Gallery

Open an Sawe Car Print an Indo Lievice	Search 🔚 Tinfiniti 🎹 Ferrer Colum	to III Hore Columns				
es	* Table Report Galery	Timeline 🛄 Disk 👘 Code				
me Entres Bookmarks & Search HRs 4		[] [] (1+6) ing7.gg	C 4 (1+7) ing5.gg	(148) ang5 tog	💷 🔛 (149) Ing9, Ipg	(150) img9.tog
Same =0= Pér Estanta 🎒 Permusiona 🗍 Refri						
		200			And Address of the owner owner owner owner own	And Address of the owner owner owner owner own
B O O MCT-MK						
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0					and the second se	
B-D CI MCT-PL					AND A DESCRIPTION OF	and the second
🖶 🌒 🔂 MCT-RU					STAR STAR	and set
B D D MCT-TR	SWI SHE					
() OT-US	(151) 122200.msp.	🗔 📑 (152) 50007 mep	(153) CID logo White1.hmp	🗔 🔜 (154) 5001c.mep	🗔 📓 (195) TR-wp4.tpg	🗔 🔛 (156) TR-wp4.3pg
G D MCT-ZA						
RSSFeed			A STATE		A DESCRIPTION OF	
These Walpaper					and the second s	
- Sorting					and the second se	
					The second s	
GIO CO DAR			CLO			
GIO IN			10 10 10 10 10 10 10 10 10 10 10 10 10 1			
🛞 🗢 💭 Enstaller	(157) mg28.jpg	(158) mg28.jpg	(159) ing5.3pg	(160) mg5 gg	(161) 32218d.msp.	[] [3 (162) wrige.brig
l2Schemas						
- Ci Cai						
Dvekennelikeparts	Shift of the second second	Sector Carls and				
🖶 🖶 🛄 Logi					150	
Heda					@N	
Original Andrewson Contents						
ModemLogs						
NAPP_Disn_Log	🗔 🔛 (163) controls.brip	(164) PL-wp5.tpg	(165) PL-405.00	🗇 🔡 (166) IT-wp1./pg	(167) IT-ep1.bg	(168) AU-wp6-lpg
a a 🖂 🚞 cem		Internet internet and stimute a part of the	Tel MAAJAGERUP CONTRACTOR CONTRACTOR			
- Citine Web Pages	a			1. Cardena and Million	Contraction Contractor	Contraction of the local division of the loc
COBEONIA	the second se		CARLES TO THE	A REAL PROPERTY AND A REAL		NUL TIME CONTRACTOR
🕀 🗃 🛄 Parther	a		27 Y Y Y	A DESCRIPTION OF THE OWNER	and a standard at the	State of the state
PCHEALTH	Married Contractory	AND AN AND AND A CAMP OF		· · · · · · · · · · · · · · · · · · ·	·····································	
🕸 🕒 🧰 Performance	100 Contraction (100 Contraction)	Service of the servic	ALL DESCRIPTION OF TAXABLE PARTY.		The second second	
PLA	~	T WTHAT AND THE REAL OF	S STATE AND TAKEN	A STATE STATE		
PolicyDefinitions	-					
t 💭 Hex 🍙 Doc 🐑 Transcript 🛄 Picture 🔅	🗄 Report 🛄 Console 🕲 Dirian 🍠 O	utput 🔲 Lock 🛄 Codepage 🗔 (0181800				EnSoupt Quers TFitters LIR Con
A LOW AND A LOW ADDRESS			-			the Pla EnScript
CONTRACTOR OF THE OWNER.						+ C C4Al vt.0.4 (released 07-Har-20
- WHAT AND BEEN						Examples
						Forensic
A state of state of the second						B-Ca Include
						Brian Main

ImeVEWIC/EU/Windows/wins/slamd64_mkrosoft-windows-photosamples_31b/3856ad364e35_6.1.7600.16385_more_f/36e0e55988042be/Koala.pp (P5 35386544 L5 10603696 CL 1325462 50 000 FO 0 LE 0)

(fstart 🙆 🧱 💌

100 10 10:17 AM

& Technology **EnCase Document View**

File	Edit	New	Tools Hel				
1	Amer III	2 min	- Channel	A faire	and Rold Designer.	C Gauge (B)	Trade and

Ņ

College of Engineering

EnCase Forensic

Cases	III Table	Report 🛄 Galary 🕑 Tanaina 🛄 Disk 🐴 Code								
Home Entries Decomments 🔍 Search Hits 🕩		Name	Fiter	In Report	File	File Type	File	Signature	Description	ls Delete
To Hone #0+ File Extents 🔒 Permesione (3)Refrit •	21	hpoat20t.onl		NO	stail	19/L Document	Document		File, Anthree, Hand United	NO .
	22	Roler.System.Summary.and		NO	and	XML Document	Document		File, Archive	NO
- Coffine Web Pages	23	🗋 hpos510k.snil		NO	sonii.	XML Document	Document		File, Archive, Hard Unked	CM1
COBCOffer	CI 24	D AppenH0Limi		NO	inc	39% Document	Document		File, Archive, Hard Linked	NO
G OCEONER	C 25	hpca430t.sml		NO	ani	1916 Document	Document		Pile, Archive, Hard United	NO
-O Lang	26	http://www.state.com		NO	scrift	XML Document	Document		File, Archive, Hard Linked	NO
🕀 🕒 🛄 res	1 27	tricipoite (NO	ionii .	XML Document	Document		File, Archive	NO
Le clongueue	28	hpsa310t.std		NO	inter i	1991L Document	Document		File, Anthree, Hard Linked	NO :
	29	hpnfill00t.sml		NO	and	XML Document	Document		File, Archive, Hard Unked	NO
	30	Tep17700t set		NO	ionii.	XML Document	Document:		File, Archive, Hard Linked	NO I
UnattendGC	31	Rules.System.Performance.cml		NO	inc	XML Document	Document.		File, Archive	NO
I POHEALTH	1 32	> Fp17600t.and		NO	oral	XML Document	Document		Pile, Archive, Hard United	NO
Deformation	30.	hpl7500e.and		NO	sonil	MML Document	Document :		File, Archive, Hard Linked	NO
E PLA	E ≫	hpt7400k.aml		NO	ioni	XML Document	Document		File, Archive, Hard Linked	NO
Peports	1 35	C Rules System Network. ml		NO	linto	1991 Document	Document		File, Archive	NO
in e Carlos	2 36	Ch Fol7300t.and		NO	imi	XML Document	Document		File, Archive, Hardtinked	NO
- System	37	Rules System NetTrace .xml		NO	ionii.	XML Document	Document		File, Archive	NO
Templates	38	hph8600t.cml		NO	linc	XP/L Document	Document		He, Archive, Hard Unked	NO _
Policy/Definitions										21

. G x

100 To 10:32 AM

🔁 Text Text Text Total Transcript 🖾 Robert 🖾 Console 🕲 Definition 🖉 Output 💭 Lock 🗔 Codepage 🗋 8/18/800 EnScript Q. Hits T Filters III Condition > . In Pa EnScript C4AE vt.0.4 (released 07-Mar-2011) Wireless Network Troubleshooter 🖶 🍋 Examples Porensi; Insert Wireless Network Troubleshooting Tables H C Include B Ca Man Create Registry Wireless Adapter Table - Source Processor 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 2 3 BREVIEWU2E(Windows)PLAI/Fulenien-L03Rules System Windows uni (P5 46354480 L3 21571632 CL 2590454 SO 000 PO 0 LE 0)

w





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



Ņ

C Carro Car

	case rolensic										Carlos Carlos		10- V
= -	🚺 Case (LTN Load Evider	nce File Test	t) 🔻 🖏 Vie	ew 🔻	帝	Too	əls 🔻 🏤 EnScript 🔻 📇 Add Evidence 🔻						0 •
(i) I	lome 🛛 🔒 Evidence 🗙 📿	🔍 Search 🛛 🛪	रो										
G	Yiewing (Search) •	Split M	lode 🕶 [[=	Con	ditior	n 🔻	🍿 Filter 💌 🐮 Searches 💌 🗢 Tags 💌 🎃 Review P	ackage 🔻 🖮 F	law Search R	esults 🔻 🚫 Bor	okmark 💌 📄	Go to file 🛛 💓 🕶 🖶	*
1.000	Index 🗟 🍝 🔣	. ►	1 0	A PROPERTY AND A	2002/14/12		Timeline Gallery			· · · · · ·	earneance the		
	▼ #_# ▼ ~ ^a A or takes and Business	673 43 6			* 7	ž↓ `	 Selected 0/156 		Eile I	122521	78	10	ei l
1916	and pustness						Name	Tag	File Ext	Logical Size	Item Type	Category	Si 🔺
					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
-	Word		Items *		67		footer[1].htm		htm	25,041	Document	Document	Matc
1	business	1,615	372		68		google_com[1].htm		htm	26,642	Document	Document	Matc
2	business'	4	3		69	0	hiding_text_in_text_steganography_project[1].htm		htm	27,967	Document	Document	Matc 🗏
3	business.com	2	1		70		110317-224244_adv_11[1].htm		htm	28,605	Document	Document	Matc
4	business2telephonenu	1	1		71		search[1].htm		htm	32,203	Document	Document	Matc
5	business_and_economy	2	2		72		2B08EC33d01			33,185	Document	Document	Alias
6	business_and_shopping	4	2		73		flashplayer[1].htm		htm	36,903	Document	Document	Matc
7	business_at_hand_idiom	1	1		74		_CACHE_003_			40,202	Document	Document	Alias
8	business_credit_cards	6	4		75		google_com[1].htm		htm	41,101	Document	Document	Matc
9	business_exchange	1	1		76		_CACHE_003_			57,135	Document	Document	Alias _
10	business_finance	2	2 +	-		lina.					- *		
	husiness	1	1										
11	Fields 📓 Report 🕍 Te	ext 🔠 Hex	iiiii Deco	de)oc	📔 Transcript 🛛 🖺 Picture 📓 Review 🖸 Consol	e					Lock
書	Find 🌺 Find Next 👔	1 📃 🗹	Compresse	ed Vie	ew		Previous Item 🛄 Next Item 📲↔ Fit To Page						
	/directory/Business												
	Business • /Directory/Business												
	Business												
	Everybody has a right to pri												
381	ife or <mark>business</mark>) from unaut	norized view	vers., Free a	owni	oaa o	or vi	ewPoint 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

	3) 🔹 🖏 View 👻 🍈 Tools 💌 🔧	EnScript		_		P Microphone	Lee Tools	
								. Gr
	ence × Q Search × S Bookn				1/2010/000	0		
		🗅 Tags 👻 🚰 Edit 🌝 Add Note 🗽 Delete	e Folder 💊 Bookmark 👻 💽 Go to	File QIFin	d Related			
D Sookmark		Table 🧐 Timeline 🎼 Gallery						
		III ▼ 21 ▼ 🗔 Selected 0/13 🚰 Edit	🌽 Add Note 🛛 🗼 Delete Folder					-
		Name	Comment	Tag	File Ext	Logical Size	Item Type	Cate
		1 🍶 Documents	The below bookmar		-		0 None	
		2 🍌 Pictures				(0 None	
		3 🍶 Email	The below bookmar			(0 None	
		4 🍶 Internet Artifacts	The below bookmar			0	0 None	
		5 🚰 Literature	Collection of literature				0 None	
	-							
] Fields 🔛 Rep	oort 🔄 Text 🔠 Hex 🇰 Decc	ode 📧 Doc 💽 Transcript 🎼 Picture						Dock 📿
	- I the second se	ode 📧 Doc 💽 Transcript 🎼 Picture						Lock
	- I the second se	ode 📧 Doc 💽 Transcript 🎼 Picture	Value					Lock
II - ≩↓ - Name	- I the second se	ode 📧 Doc 💽 Transcript 🎼 Picture	Value					Lock
□ - 2 ↓ -	oort 📩 Text 👸 Hex 🗰 Deco	nde 📧 Doc 💽 Transcript 🎼 Picture						Lock
III ← 2 ↓ ← Name Name Comment Tag	oort 📩 Text 👸 Hex 🗰 Deco							Lock
II ← ≩↓ ← Name Name Comment Tag	oort 📩 Text 👸 Hex 🗰 Deco							
III ▼ 22↓ ▼ Name S> Name	oort 📩 Text 👸 Hex 🗰 Deco							

Deleted Files

	1		
💫 exFAT.E01	05/25/10 01:15:30PM	05/25/10 01:16:00PM	05/25/10 01:16:00PM
💫 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
💫 ReadyBoostPerfTest.tmp	06/25/10 10:00:16AM	06/25/10 10:00:14AM	06/25/10 10:00:16AM
BDT (UTC-4hrs).txt	06/25/10 10:00:24AM	06/25/10 10:00:24AM	06/25/10 10:00:24AM
Deleted.txt	05/25/10 01:09:56PM	05/25/10 01:09:42PM	05/25/10 01:09:56PM
D UTC.txt	06/25/10 03:00:58PM	06/25/10 03:00:58PM	06/25/10 03:00:58PM
Berlin (UTC+1hr).txt	06/25/10 04:01:40PM	06/25/10 04:01:40PM	06/25/10 04:01:40PM
💭 Kathmandu (UTC+5.45hr).txt	06/25/10 07:47:20PM	06/25/10 07:47:20PM	06/25/10 07:47:20PM
EDT (UTC-4hrs).txt	06/25/10 10:04:32AM	06/25/10 10:04:32AM	06/25/10 10:04:32AM
D. New Text Document.txt	06/25/10 02:05:32PM	06/25/10 02:05:32PM	06/25/10 02:05:32PM
UTC.txt	06/25/10 02:05:32PM	06/25/10 02:05:32PM	06/25/10 02:05:32PM
Berlin Time (UTC+1hr).txt	06/25/10 04:06:12PM	06/25/10 04:06:12PM	06/25/10 04:06:12PM
🗋 Kathmandu (UTC+5.45hr).txt	06/25/10 07:51:58PM	06/25/10 07:51:58PM	06/25/10 07:51:58PM
BobbyHelmsLyrics.txt	05/25/10 01:07:56PM	05/25/10 01:08:56PM	05/25/10 01:08:56PM
New Text Document.txt	06/25/10 03:00:58PM	06/25/10 03:00:58PM	06/25/10 03:00:58PM
	 exFAT (Extended FAT)-Hamm-5-26-201 ReadyBoostPerfTest.tmp EDT (UTC-4hrs).txt Deleted.txt UTC.txt Berlin (UTC+1hr).txt Kathmandu (UTC+5.45hr).txt EDT (UTC-4hrs).txt New Text Document.txt UTC.txt Berlin Time (UTC+1hr).txt Kathmandu (UTC+5.45hr).txt Berlin Time (UTC+1hr).txt Kathmandu (UTC+5.45hr).txt 	Image: SexFAT (Extended FAT)-Hamm-5-26-201 03/27/10 12:26:26PM Image: ReadyBoostPerfTest.tmp 06/25/10 10:00:16AM Image: EDT (UTC-4hrs).txt 06/25/10 10:00:24AM Image: Deleted.txt 05/25/10 01:09:56PM Image: Deleted.txt 06/25/10 03:00:58PM Image: Deleted.txt 06/25/10 04:01:40PM Image: Deleted.txt 06/25/10 04:01:40PM Image: Deleted.txt 06/25/10 07:47:20PM Image: Deleted.txt 06/25/10 02:05:32PM Image: Deleted.txt 06/25/10 02:05:32PM Image: Deleted.txt 06/25/10 02:05:32PM Image: Deleted.txt 06/25/10 04:06:12PM Image: Deleted.txt 06/25/10 04:06:12PM Image: Deleted.txt 06/25/10 04:06:12PM Image: Deleted.txt 06/25/10 04:06:12PM Image: Deleted.txt 06/25/10 07:51:58PM Image: Deleted.txt 06/25/10 07:51:58PM	exFAT (Extended FAT)-Hamm-5-26-201 03/27/10 12:26:26PM 05/25/10 01:09:18PM ReadyBoostPerfTest.tmp 06/25/10 10:00:16AM 06/25/10 10:00:14AM EDT (UTC-4hrs).txt 06/25/10 10:00:24AM 06/25/10 10:00:24AM Deleted.txt 05/25/10 01:09:56PM 05/25/10 01:09:42PM UTC.txt 06/25/10 03:00:58PM 06/25/10 03:00:58PM Berlin (UTC+1hr).txt 06/25/10 07:47:20PM 06/25/10 07:47:20PM Kathmandu (UTC+5.45hr).txt 06/25/10 02:05:32PM 06/25/10 02:05:32PM New Text Document.txt 06/25/10 02:05:32PM 06/25/10 02:05:32PM UTC.txt 06/25/10 04:01:40PM 06/25/10 02:05:32PM UTC.txt 06/25/10 02:05:32PM 06/25/10 02:05:32PM UTC.txt 06/25/10 02:05:32PM 06/25/10 02:05:32PM UTC.txt 06/25/10 02:05:32PM 06/25/10 02:05:32PM UTC.txt 06/25/10 04:06:12PM 06/25/10 04:06:12PM Berlin Time (UTC+1hr).txt 06/25/10 07:51:58PM 06/25/10 07:51:58PM Kathmandu (UTC+5.45hr).txt 06/25/10 07:51:58PM 06/25/10 07:51:58PM BobbyHelmsLyrics.txt 05/25/10 01:07:56PM 05/25/10 01:08:56PM

EIC2010 (F:)

Ņ

College of Engineering

✓ 4→ Search CEIC201

New folder Burn -Date modified Type Size Name Berlin Time (UTC+1hr).txt Text Document 6/25/2010 10:06 AM 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-computerforensics-tool/article/195999/
- http://www.law.com/jsp/lawtechnologynews/PubA rticleLTN.jsp?id=1202584495563&Product_Review _Encase_Forensic_7&slreturn=20130405160529
- https://www.ncjrs.gov/pdffiles1/nij/183451.pdf
- http://www.westwood.edu/programs/school-oftechnology/computer-forensics-online-degree/lawenforcement-computer-forensics
- <u>Computer Forensics: Info Sec Pro Guide</u>
- <u>Security Guide to Network Security Fundamentals</u>



Questions?