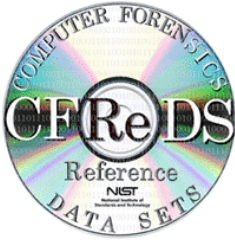**NIST CFReDS Project**

(Computer Forensic Reference Data Sets)

NIST CFReDS:

Data Leakage Case

Software and Systems Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899

July 23, 2018

NIST

**National Institute of
Standards and Technology**

U.S. Department of Commerce

Table of Contents

1. SCENARIO OVERVIEW

'Iaman Informant' was working as a manager of the technology development division at a famous international company OOO that developed state-of-the-art technologies and gadgets.

One day, at a place which 'Mr. Informant' visited on business, he received an offer from 'Spy Conspirator' to leak of sensitive information related to the newest technology. Actually, 'Mr. Conspirator' was an employee of a rival company, and 'Mr. Informant' decided to accept the offer for large amounts of money, and began establishing a detailed leakage plan.

'Mr. Informant' made a deliberate effort to hide the leakage plan. He discussed it with 'Mr. Conspirator' using an e-mail service like a business relationship. He also sent samples of confidential information though personal cloud storage.

After receiving the sample data, 'Mr. Conspirator' asked for the direct delivery of storage devices that stored the remaining (large amounts of) data. Eventually, 'Mr. Informant' tried to take his storage devices away, but he and his devices were detected at the security checkpoint of the company. And he was suspected of leaking the company data.

At the security checkpoint, although his devices (a USB memory stick and a CD) were briefly checked (protected with portable write blockers), there was no evidence of any leakage. And then, they were immediately transferred to the digital forensics laboratory for further analysis.

The information security policies in the company include the following:

(1) Confidential electronic files[1] should be stored and kept in the authorized external storage devices and the secured network drives.
(2) Confidential paper documents and electronic files can be accessed only within the allowed time range from 10:00 AM to 16:00 PM with the appropriate permissions.
(3) Non-authorized electronic devices such as laptops, portable storages, and smart devices cannot be carried onto the company.
(4) All employees are required to pass through the 'Security Checkpoint' system.
(5) All storage devices such as HDD, SSD, USB memory stick, and CD/DVD are forbidden under the 'Security Checkpoint' rules.

In addition, although the company managed separate internal and external networks and used DRM (Digital Rights Management) / DLP (Data Loss Prevention) solutions for their information security, 'Mr. Informant' had sufficient authority to bypass them. He was also very interested in IT (Information Technology), and had a slight knowledge of digital forensics.

In this scenario, find any evidence of the data leakage, and any data that might have been generated from the suspect's electronic devices.

---

[1] All the seed files (confidential files used in the scenario) were created based on MS Office files randomly selected from Govdocs1 (https://digitalcorpora.org/corpora/files). The seed files are available online at NIST/CFReDS web-site.

2. TARGET SYSTEMS AND DEVICES

Target		Detailed Information		Note
Personal Computer (PC)	HW	Type	Virtual System	VMWare v11
		CPU	1 Processer (2 Core)	
		RAM	2,048 MB	
		HDD Size	20 GB	
		File System	NTFS	
		IP Address	10.11.11.129	NAT
	SW (OS)	Operating System	Microsoft Windows 7 Ultimate (SP1)	English (64 bits) MSDN image[2] (not activated)
	SW (Apps)	Web	- MS Internet Explorer - Google Chrome	Latest versions if possible
		Document	Microsoft Office	Word, Excel, PowerPoint MSDN image[3] (not activated)
		Cloud	- Google Drive - Apple iCloud	Auto Syncing is ON if possible
		E-mail	Microsoft Outlook	NIST.gov mail server[4]
		Anti-forensics	- CCleaner - Eraser	Latest versions if possible
Removable Media #1 (RM#1)[5]	HW	Type	USB removable storage device	
		Mfg.	SanDisk	Vendor ID = 0x0781
		Model	Cruzer Fit	
		Serial No.	4C530012450531101593	Unique serial number
		Size	4 GB	
		File System	exFAT	
		Volume label	Authorized USB	
Removable Media #2 (RM#2)	HW	Type	USB removable storage device	
		Mfg.	SanDisk	Vendor ID = 0x0781
		Model	Cruzer Fit	
		Serial No.	4C530012550531106501	Unique serial number
		Size	4 GB	Partitioned 1 GB only
		File System	FAT32	
		Volume label	IAMAN $_@	
Removable Media #3 (RM#3)	HW	Type	CD-R	
		Size	700 MB	
		File System	UDF	Created by Windows 7
		Volume label	IAMAN CD	
Smart Device	-	-	-	Future work[6]

---

[2] SHA-1 hash value: `1693B6CB50B90D96FC3C04E4329604FEBA88CD51`

[3] SHA-1 hash value: `377F1F97DBE99104CF053DF3632377F07C9310C7`

[4] NIST e-mail accounts: iaman.informant@nist.gov, spy.conspirator@nist.gov

[5] Authorized USB memory stick (← confidential electronic files of the company)

[6] Smart devices and Apple OS X system can be considered in the future work.

3. DETAILED BEHAVIOR OF THE SUSPECT

Regarding developing user and system artifacts, we tried to keep simple as much as possible. For efficiency of both developing and analyzing images, it was designed to avoid complicated operations and create various meaningful artifacts from the viewpoint of digital forensics.

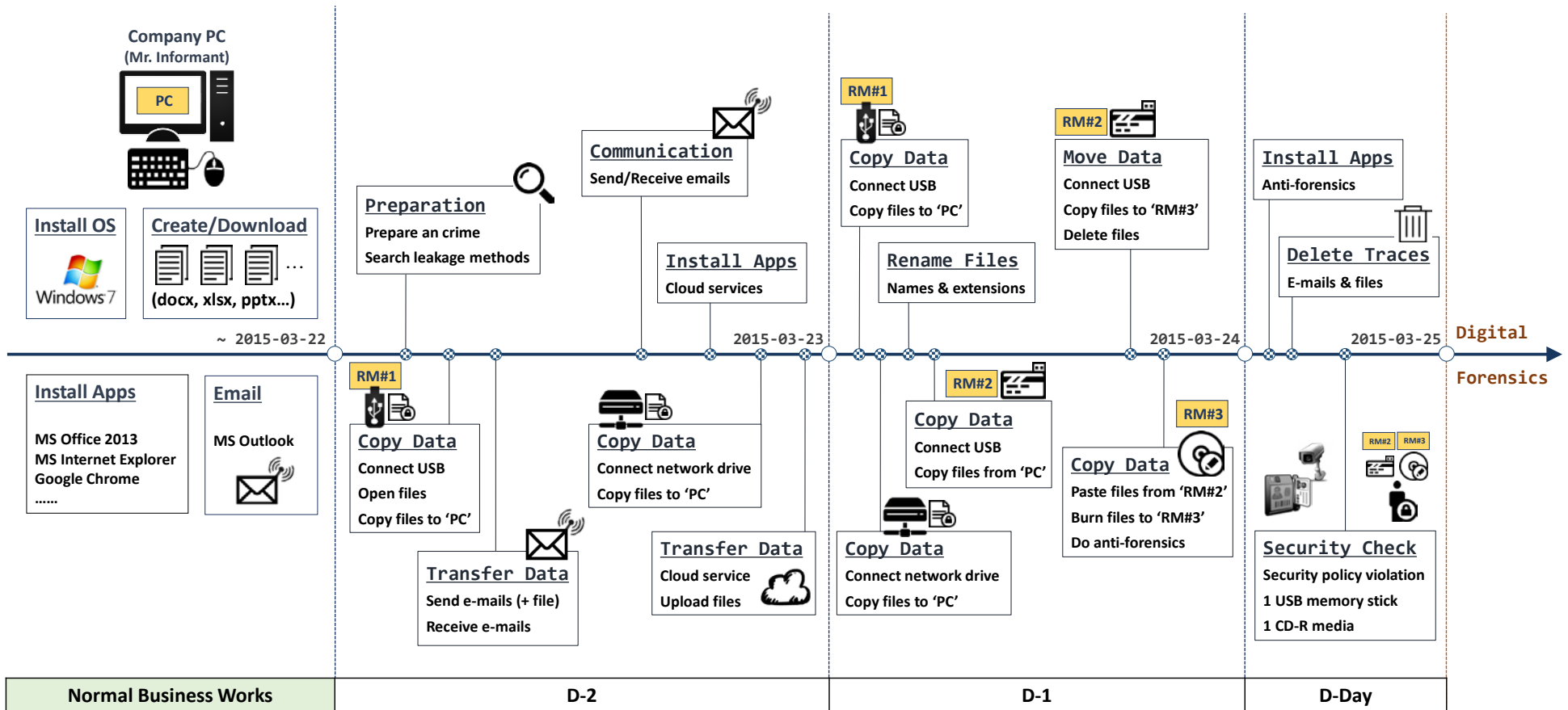Detailed behavior of the suspect is described as a text (below table) and visual diagram.

Step	Date/Time	Action	Additional Description	Note
Normal	~ 2015-03-22	Install OS	Windows 7 Ultimate	
		Configure settings	Set the timezone to (UTC-05) Eastern Time	
		Install Apps	(1) Microsoft Office (2) Microsoft Internet Explorer (3) Google Chrome	Latest versions if possible
		Create/Download business data	Electronic documents (Word, Excel, PowerPoint…)	Company's common files
		Email	Microsoft Outlook with NIST e-mail account	iaman.informant@nist.gov
		Create user accounts	"admin11" → login count: 2 "ITechTeam" → login count: 0 "temporary" → login count: 1	
D-2	2015-03-23 13:29	Receive an e-mail	spy.conspirator@nist.gov → iaman.informant@nist.gov	[Subject: Hello, Iaman] "How are you doing?"
	2015-03-23 14:01 ~ 2015-03-23 14:21	Prepare a crime (data leakage)	Searching the leakage methods through web-browsers: - Microsoft Internet Explorer - Google Chrome	Google, Bing search engine --- Chrome 1) data leakage methods 2) leaking confidential information 3) information leakage cases 4) intellectual property theft 5) how to leak a secret --- IE 11 6) file sharing and tethering 7) DLP DRM 8) e-mail investigation 9) what is windows system artifacts 10) investigation on windows machine 11) windows event logs 12) cd burning method in Windows 13) external device and forensics --- Chrome 14) cloud storage 15) digital forensics 16) how to delete data 17) anti-forensics 18) system cleaner 19) how to recover data 20) data recovery tools
	2015-03-23 14:31	Connect USB	'RM#1' USB memory stick	
	2015-03-23 14:36	Search keywords	Searching confidential data using Windows Search function	Keyword: "secret"
	2015-03-23 14:37	Open files	[secret_project]_proposal.docx [secret_project]_design_concept.ppt	Open and read files
	2015-03-23 14:39	Copy & open files	Copying confidential files from 'RM#1' to 'PC'	"\Desktop\S data"
			[RM#1] RM#1\Secret Project Data\proposal\[secret_project]_proposal.docx RM#1\Secret Project Data\design\[secret_project]_design_concept.ppt	[PC] %UserProfile%\Desktop\S data\[secret_project]_proposal.docx %UserProfile%\Desktop\S data\[secret_project]_design_concept.ppt
	2015-03-23 14:39	Disconnect USB	Ejecting 'RM#1'	
	2015-03-23 14:39	Configure settings	Show 'file name extensions' in Windows Explorer	
	2015-03-23 14:41	Rename files	All names and extensions are changed (e.g., xlsx → jpg, docx → mp3…)	[secret_project]_detailed_proposal.docx → landscape.png [secret_project]_design_concept.ppt → space_and_earth.mp4

	2015-03-23 14:44	Send an e-mail	iaman.informant@nist.gov → spy.conspirator@nist.gov	"Successfully secured."
	2015-03-23 15:14	Receive an e-mail	spy.conspirator@nist.gov → iaman.informant@nist.gov	[Subject: Good job, buddy] "Good, job. I need a more detailed data about this business."
	2015-03-23 15:19	Send an e-mail	iaman.informant@nist.gov → spy.conspirator@nist.gov	"This is a sample." (space_and_earth.mp4)
	2015-03-23 15:20	Receive an e-mail	spy.conspirator@nist.gov → iaman.informant@nist.gov	"Okay, I got it. I'll be in touch."
	2015-03-23 15:26	Receive an e-mail	spy.conspirator@nist.gov → iaman.informant@nist.gov	[Subject: Important request] "I confirmed it. But, I need a more data. Do your best."
	2015-03-23 15:27	Send an e-mail	iaman.informant@nist.gov → spy.conspirator@nist.gov	"Umm… I need time to think."
	2015-03-23 16:00	Search and download Apps	Searching cloud storage services using Chrome	
	2015-03-23 16:00	Install Apps	(1) Google Drive (2) Apple iCloud	
	2015-03-23 16:05	Login cloud service	Login Google Drive service with an account (iaman.informant.personal@gmail.com)	
	2015-03-23 16:23	Connect network drive	Connecting secured shared network drive	\\10.11.11.128\secured_drive
	2015-03-23 16:24	Search files	Traversing directories and files using Windows Explorer	
	2015-03-23 16:26	Connect network drive	Mapping network drive (v:)	\\10.11.11.128\secured_drive
	2015-03-23 16:26	Open files	(secret_project)_pricing_decision.xlsx [secret_project]_final_meeting.pptx	Open and read files
	2015-03-23 16:28	Copy & open files	Copying confidential files from a network drive to 'PC'	"\Desktop\S data"
			[Network Drive] Secret Project Data\pricing decision\(secret_project)_pricing_decision.xlsx Secret Project Data\final\[secret_project]_final_meeting.pptx	[PC] %UserProfile%\Desktop\S data\(secret_project)_pricing_decision.xlsx %UserProfile%\Desktop\S data\[secret_project]_final_meeting.pptx
	2015-03-23 16:29	Disconnect network drive	Unmapping network drive (v:)	\\10.11.11.128\secured_drive
	2015-03-23 16:30	Rename files	All names and extensions are changed (e.g., xlsx → jpg, docx → mp3…)	(secret_project)_pricing_decision.xlsx → happy_holiday.jpg [secret_project]_final_meeting.pptx → do_u_wanna_build_a_snow_man.mp3
	2015-03-23 16:32	Upload files	Uploading some files to Google Drive and sharing them	happy_holiday.jpg do_u_wanna_build_a_snow_man.mp3
	2015-03-23 16:38	Send an e-mail	iaman.informant@nist.gov → spy.conspirator@nist.gov	[Subject: It's me] "Use links below."
	2015-03-23 16:41	Receive an e-mail	spy.conspirator@nist.gov → iaman.informant@nist.gov	"I got it."
	2015-03-23 16:42	Delete files	Deleting files from Google Drive	
	2015-03-23 16:43	Misc.	Personal web-browsing using IE	During approx. 15 minutes
D-1	2015-03-24 09:26	Receive an e-mail	spy.conspirator@nist.gov → iaman.informant@nist.gov	[Subject: Last request] "This is the last request. I want to get the remaining data."
	2015-03-24 09:30	Send an e-mail	iaman.informant@nist.gov → spy.conspirator@nist.gov	"Stop it! It is very hard to transfer all data over the internet!"
	2015-03-24 09:33	Receive an e-mail	spy.conspirator@nist.gov → iaman.informant@nist.gov	"No problem. U can directly deliver storage devices that stored it."
	2015-03-24 09:35	Send an e-mail	iaman.informant@nist.gov → spy.conspirator@nist.gov	"This is the last time.."
	2015-03-24 09:38	Connect USB	'RM#1' USB memory stick	
	2015-03-24 09:40	Copy files	Copying confidential files 'RM#1' to 'PC'	
			[RM#1] RM#1\Secret Project Data\design\[secret_project]_design_concept.ppt RM#1\Secret Project Data\design\[secret_project]_detailed_design.pptx RM#1\Secret Project Data\design\[secret_project]_revised_points.ppt RM#1\Secret Project Data\proposal\[secret_project]_detailed_proposal.docx RM#1\Secret Project Data\proposal\[secret_project]_proposal.docx	[PC] %UserProfile%\Desktop\S data\Secret Project Data\design\[secret_project]_design_concept.ppt %UserProfile%\Desktop\S data\Secret Project Data\design\[secret_project]_detailed_design.pptx %UserProfile%\Desktop\S data\Secret Project Data\design\[secret_project]_revised_points.ppt %UserProfile%\Desktop\S data\Secret Project Data\proposal\[secret_project]_detailed_proposal.docx %UserProfile%\Desktop\S data\Secret Project Data\proposal\[secret_project]_proposal.docx

	2015-03-24 09:40	Disconnect USB	Ejecting 'RM#1'	
	2015-03-24 09:47	Connect network drive	Secured shared network drive	\\10.11.11.128\secured_drive
	2015-03-24 09:47	Copy files	Copying confidential files from a network drive to 'PC'	

[Network Drive]	[PC]
Secret Project Data\design\[secret_project]_detailed_design.pptx	%UserProfile%\Desktop\S data\Secret Project Data\design\[secret_project]_detailed_design.pptx
Secret Project Data\final\[secret_project]_final_meeting.pptx	%UserProfile%\Desktop\S data\Secret Project Data\final\[secret_project]_final_meeting.pptx
Secret Project Data\pricing decision\[secret_project]_market_analysis.xlsx	%UserProfile%\Desktop\S data\Secret Project Data\pricing decision\[secret_project]_market_analysis.xlsx
Secret Project Data\pricing decision\[secret_project]_market_shares.xls	%UserProfile%\Desktop\S data\Secret Project Data\pricing decision\[secret_project]_market_shares.xls
Secret Project Data\pricing decision\[secret_project]_price_analysis_#1.xlsx	%UserProfile%\Desktop\S data\Secret Project Data\pricing decision\[secret_project]_price_analysis_#1.xlsx
Secret Project Data\pricing decision\[secret_project]_price_analysis_#2.xls	%UserProfile%\Desktop\S data\Secret Project Data\pricing decision\[secret_project]_price_analysis_#2.xls
Secret Project Data\pricing decision\[secret_project]_pricing_decision.xlsx	%UserProfile%\Desktop\S data\Secret Project Data\pricing decision\[secret_project]_pricing_decision.xlsx
Secret Project Data\progress\[secret_project]_progress_#1.docx	%UserProfile%\Desktop\S data\Secret Project Data\progress\[secret_project]_progress_#1.docx
Secret Project Data\progress\[secret_project]_progress_#2.doc	%UserProfile%\Desktop\S data\Secret Project Data\progress\[secret_project]_progress_#2.docx
Secret Project Data\progress\[secret_project]_progress_#3.doc	%UserProfile%\Desktop\S data\Secret Project Data\progress\[secret_project]_progress_#3.doc
Secret Project Data\proposal\[secret_project]_detailed_proposal.docx	%UserProfile%\Desktop\S data\Secret Project Data\proposal\[secret_project]_detailed_proposal.docx
Secret Project Data\technical review\[secret_project]_technical_review_#1.docx	%UserProfile%\Desktop\S data\Secret Project Data\technical review\[secret_project]_technical_review_#1.docx
Secret Project Data\technical review\[secret_project]_technical_review_#1.pptx	%UserProfile%\Desktop\S data\Secret Project Data\technical review\[secret_project]_technical_review_#1.pptx
Secret Project Data\technical review\[secret_project]_technical_review_#2.docx	%UserProfile%\Desktop\S data\Secret Project Data\technical review\[secret_project]_technical_review_#2.docx
Secret Project Data\technical review\[secret_project]_technical_review_#2.ppt	%UserProfile%\Desktop\S data\Secret Project Data\technical review\[secret_project]_technical_review_#2.ppt
Secret Project Data\technical review\[secret_project]_technical_review_#3.doc	%UserProfile%\Desktop\S data\Secret Project Data\technical review\[secret_project]_technical_review_#3.doc
Secret Project Data\technical review\[secret_project]_technical_review_#3.ppt	%UserProfile%\Desktop\S data\Secret Project Data\technical review\[secret_project]_technical_review_#3.ppt

Time	Action	Description	Detail
2015-03-24 09:50 ~ 2015-03-24 09:56	Rename files	All names and extensions are changed (20 files in "%UserProfile%\Desktop\S data\ Secret Project Data\")	(secret_project)_market_analysis.xlsx → new_years_day.jpg [secret_project]_progress_#3.doc → my_friends.svg
2015-03-24 09:58	Connect USB	'RM#2' USB memory stick	
2015-03-24 09:59	Copy files	Copying confidential files to 'RM#2'	Copy a directory "%UserProfile%\ Desktop\S data\Secret Project Data\" including sub-dirs and files to RM#2
2015-03-24 10:00	Verify files	Traversing directories and files in 'RM#2' using Windows Explorer	Open a file (winter_whether_advisory.zip)
2015-03-24 10:02	Disconnect USB	Ejecting 'RM#2'	
2015-03-24 10:07	Delete files	Deleting directories and files from 'PC'	"\Desktop\S data" Normal deletion: [Shift] + [Delete]
2015-03-24 10:07	Misc.	Personal web-browsing and searching anti-forensic methods (Chrome, IE)	During approx. 4 hours
2015-03-24 14:28	Misc.	Launching a game ('Solitaire')	
2015-03-24 14:31	Misc.	Launching the sticky note and writing text	
2015-03-24 14:32	Misc.	Creating a letter of resignation (.docx)	During approx. 30 minutes Windows Desktop
2015-03-24 15:32	Receive an e-mail	spy.conspirator@nist.gov → iaman.informant@nist.gov	[Subject: Watch out!] "USB device may be easily detected. So, try another method."
2015-03-24 15:34	Send an e-mail	iaman.informant@nist.gov → spy.conspirator@nist.gov	"I am trying."
2015-03-24 15:38	Connect USB	'RM#2' USB memory stick	
2015-03-24 15:40	Practice CD burning	Testing CD-R burning process and preparing meaningless files for anti-forensics	During approx. 55 minutes "\Desktop\temp" (1 exe, 8 images)
2015-03-24 16:40	Insert CD	CD-R	Windows CD Burning Type 2: With a CD/DVD/ player (Mastered)
2015-03-24 16:40	Copy files	Copying confidential files from 'RM#2' to CD-R	With renaming directories: - design → de - pricing decision → pd - progress → prog - proposal → prop - technical review →tr
2015-03-24 16:41	Burn files	Burning confidential files to CD-R	
2015-03-24 16:44	Verify files	Traversing directories and files in CD-R using Windows Explorer	
2015-03-24 16:44	Format disk	Formatting the CD-R as an empty disk	
2015-03-24 16:45	Copy files	Copying and burning meaningless files to CD-R in order for creating a new session	Anti-forensics
2015-03-24 16:53	Insert CD	CD-R (new one)	Windows CD Burning Type 1: Like a USB flash drive

	2015-03-24 16:54	Copy files	Copying and burning confidential files from 'RM#2' to CD-R	
	2015-03-24 16:55	Rename directories	Renaming directories in CD-R	
	2015-03-24 16:57	Copy files	Copying 3 meaningless files to CD-R	Koala.jpg Penguins.jpg Tulips.jpg
	2015-03-24 16:58	Delete files	Deleting confidential files from CD-R	
	2015-03-24 17:01	Verify files	Traversing directories and files in CD-R using Windows Explorer	
	2015-03-24 17:02	Delete files	Deleting copied files from 'RM#2' (Quick format)	Anti-forensics
	2015-03-24 17:03	Disconnect USB	Ejecting 'RM#2'	
	2015-03-24 17:05	Send an e-mail	iaman.informant@nist.gov → spy.conspirator@nist.gov	[Subject: Done] "It's done. See you tomorrow."
	2015-03-24 17:06	Search keywords	Searching keywords using Chrome	"security checkpoint CD-R"
D-Day	2015-03-25 10:46	Search and download Apps	Searching apps for anti-forensics using IE	Anti-forensic tools, eraser, ccleaner…
	2015-03-25 10:50	Install Apps	(1) Eraser (with .NET Framework) (2) CCleaner	During approx. 8 minutes
	2015-03-25 11:00	Delete e-mails	Deleting some e-mails in Outlook	Anti-forensics (9 emails are deleted, and 4 items of them remain in Deleted Items folder.) During approx. 10 minutes
	2015-03-25 11:13	Delete traces	Running anti-forensic tools and deleting some files	Wiping "\Desktop\temp" directory using Eraser
	2015-03-25 11:14	Delete traces	Emptying the Recycle Bin	
	2015-03-25 11:15	Delete traces	Deleting downloaded installer files (Eraser, CCleaner)	Normal deletion: [Shift] + [Delete]
	2015-03-25 11:15	Delete traces	Launching CCleaner	And then, the app was closed after doing nothing
	2015-03-25 11:18	Delete Apps	Uninstalling some Apps	CCleaner, iCloud During approx. 2 minutes
	2015-03-25 11:22	Delete traces	Launching Google Drive app and disconnecting an account	Logout from Google Drive
	2015-03-25 11:23	Delete traces	Cleaning and arranging Windows desktop	Directories and icons in Windows Desktop
	2015-03-25 11:24	Open files	Opening the resignation letter (.docx)	Windows Desktop
	2015-03-25 11:28	Print files	Printing the document to the MS XPS file and reviewing it with MS XPS viewer	
	2015-03-25 11:30	Finish works	Turning off the system and trying to go outside with 'RM#2' and 'RM#3'	RM#3 is one of two CD-Rs

Graphical Timeline of the Data Leakage Scenario

Company PC (Mr. Informant)

PC

Install OS

Windows 7

Create/Download

(docx, xlsx, pptx…)

Preparation

Prepare an crime
Search leakage methods

Communication

Send/Receive emails

Install Apps

Cloud services

Copy Data [RM#1]

Connect USB
Copy files to 'PC'

Rename Files

Names & extensions

Move Data [RM#2]

Connect USB
Copy files to 'RM#3'
Delete files

Install Apps

Anti-forensics

Delete Traces

E-mails & files

~ 2015-03-22   2015-03-23   2015-03-24   2015-03-25   **Digital**

Forensics

Install Apps

MS Office 2013
MS Internet Explorer
Google Chrome
……

Email

MS Outlook

Copy Data [RM#1]

Connect USB
Open files
Copy files to 'PC'

Transfer Data

Send e-mails (+ file)
Receive e-mails

Copy Data

Connect network drive
Copy files to 'PC'

Transfer Data

Cloud service
Upload files

Copy Data [RM#2]

Connect USB
Copy files from 'PC'

Copy Data

Connect network drive
Copy files to 'PC'

Copy Data [RM#3]

Paste files from 'RM#2'
Burn files to 'RM#3'
Do anti-forensics

Security Check

Security policy violation
1 USB memory stick
1 CD-R media

Normal Business Works	D-2	D-1	D-Day

4. ACQUIRED DATA INFORMATION

4.1. PERSONAL COMPUTER (PC) – 'DD' IMAGE

Item	Detailed Information
Filename	cfreds_2015_data_leakage_pc
MD5	A49D1254C873808C58E6F1BCD60B5BDE
SHA-1	AFE5C9AB487BD47A8A9856B1371C2384D44FD785
Imaging S/W	FTK Imager 3.4.0.1
Image Format	DD converted from VMDK (Some sectors were scrubbed[7])
Compression	Best (Smallest)
Bytes per Sector	512
Total Sectors	41,943,040
Total Size	20.00 GB (21,474,836,480 bytes)
Compressed Size	5.05 GB (5,427,795,228 bytes) ← compressed by 7zip

4.2. PERSONAL COMPUTER (PC) – 'ENCASE' IMAGE

Item	Detailed Information
Filename	cfreds_2015_data_leakage_pc
MD5	A49D1254C873808C58E6F1BCD60B5BDE
SHA-1	AFE5C9AB487BD47A8A9856B1371C2384D44FD785
Imaging S/W	EnCase Imager 7.10.00.103
Image Format	E01 (Expert Witness Compression Format) converted from above DD image
Compression	Best (Smallest)
Bytes per Sector	512
Total Sectors	41,943,040
Total Size	20.00 GB (21,474,836,480 bytes)
Compressed Size	7.28 GB (7,825,209,454 bytes)

---

[7] Unnecessary data (a group of sectors) were scrubbed manually. It was nothing to do with this scenario.

4.3. REMOVABLE MEDIA #1 (RM#1) – 'ENCASE' IMAGE

Item	Detailed Information
Filename	cfreds_2015_data_leakage_rm#1
MD5	8BFA4230BF4E35DB966B8C1A9321A0B1
SHA-1	F6BB840E98DD7C325AF45539313FC3978FFF812C
Imaging S/W	FTK Imager 3.3.0.5 (write-blocked by Tableau USB Bridge T8-R2)
Image Format	E01 (Expert Witness Compression Format)
Compression	Best (Smallest)
Bytes per Sector	512
Total Sectors	7,821,312
Total Size	3.7 GB (4,004,511,744 bytes)
Compressed Size	74.5 MB (78,186,742 bytes)

4.4. REMOVABLE MEDIA #2 (RM#2) – 'DD' IMAGE

Item	Detailed Information
Filename	cfreds_2015_data_leakage_rm#2
MD5	B4644902ACAB4583A1D0F9F1A08FAA77
SHA-1	048961A85CA3ECED8CC73F1517442D31D4DCA0A3
Imaging S/W	FTK Imager 3.3.0.5 (write-blocked by Tableau USB Bridge T8-R2)
Image Format	E01 (Expert Witness Compression Format)
Compression	Best (Smallest)
Bytes per Sector	512
Total Sectors	7,821,312
Total Size	3.7 GB (4,004,511,744 bytes)
Compressed Size	219 MB (229,899,285 bytes) ← compressed by 7zip

4.5. REMOVABLE MEDIA #2 (RM#2) – 'ENCASE' IMAGE

Item	Detailed Information
Filename	cfreds_2015_data_leakage_rm#2
MD5	B4644902ACAB4583A1D0F9F1A08FAA77
SHA-1	048961A85CA3ECED8CC73F1517442D31D4DCA0A3
Imaging S/W	EnCase Imager 7.09.00.111 (write-blocked by Tableau USB Bridge T8-R2)
Image Format	E01 (Expert Witness Compression Format)
Compression	Best (Smallest)
Bytes per Sector	512
Total Sectors	7,821,312
Total Size	3.7 GB (4,004,511,744 bytes)
Compressed Size	243 MB (255,051,328 bytes)

4.6. REMOVABLE MEDIA #3 (RM#3) – 'RAW / CUE' IMAGE

Item	Detailed Information
Filename	cfreds_2015_data_leakage_rm#3_type1
MD5	858C7250183A44DD83EB706F3F178990
SHA-1	471D3EEDCA9ADD872FC0708297284E1960FF44F8
Imaging S/W	FTK Imager 3.3.0.5
Image Format	RAW ISO / CUE (sometime BIN / CUE)[8]
Bytes per Sector	2,048
Total Sectors	52,514
Total Size	102.57 MB (107,548,672 bytes)
Compressed Size	92.8 MB (97,311,442 bytes) ← compressed by 7zip

4.7. REMOVABLE MEDIA #3 (RM#3) – 'DD' IMAGE

Item	Detailed Information
Filename	cfreds_2015_data_leakage_rm#3_type2
MD5	858C7250183A44DD83EB706F3F178990
SHA-1	471D3EEDCA9ADD872FC0708297284E1960FF44F8
Imaging S/W	FTK Imager 3.3.0.5 + bchunk[9]
Image Format	DD converted from 'RAW + CUE' using bchunk
Bytes per Sector	2,048
Total Sectors	52,514
Total Size	102.57 MB (107,548,672 bytes)
Compressed Size	78.6 MB (82,511,830 bytes) ← compressed by 7zip

4.8. REMOVABLE MEDIA #3 (RM#3) – 'ENCASE' IMAGE

Item	Detailed Information
Filename	cfreds_2015_data_leakage_rm#3_type3
MD5	DF914108FB3D86744EB688EBA482FBDF
SHA-1	7F3C2EB1F1E2DB97BE6E963625402A0E362A532C
Imaging S/W	EnCase Imager 7.09.00.111
Image Format	E01 (Expert Witness Compression Format)
Compression	Best (smallest)
Bytes per Sector	2,048
Total Sectors	52,513
Total Size	102.56 MB (107,546,624 bytes)
Compressed Size	90.21 MB (94,594,894 bytes)
Read Errors (Sector No.)	(321), (51,213), (51,233), (51,244), (51,265), (51,276), (51,297), (51,308), (51,329), (51,340), (51,361), (51,372), (51,393), (52,472), (52,481), (52,500)

---

[8] The RAW ISO file is a raw sector-by-sector binary copy of tracks in the original disk, and the CUE file is a plain-text file which stores the information of disk and tracks.

[9] bchunk v1.2.0 - BinChunker for Unix / Linux (http://he.fi/bchunk/)

5. DIGITAL FORENSICS PRACTICE POINTS

The followings are the summary of detailed practice points related to above images.

Practice Point	Description	Note

Understanding Types of Data Leakage	- Storage devices
	  ✓ HDD (Hard Disk Drive)
	  ✓ SSD (Solid State Drive)
	  ✓ USB flash drive
	  ✓ Flash memory cards
	  ✓ CD/DVD (with Optical Disk Drive)
	- Network Transmission
	  ✓ File sharing
	  ✓ Remote Desktop Connection
	  ✓ E-mail
	  ✓ SNS (Social Network Service)
	  ✓ Cloud services
	  ✓ Messenger
	* Underlined parts are covered on this image
		- Interfaces
		  ✓ ATA
		  ✓ SATA, eSATA
		  ✓ USB
		  ✓ IEEE 1394
		
		- Network interfaces
		  ✓ Ethernet cable
		  ✓ Wi-Fi
		  ✓ Bluetooth
		
		- Note
		  ✓ Tethering

Windows Forensics	- Windows event logs - Opened files and directories - Application (executable) usage history - CD/DVD burning records - External devices attached to PC - Network drive connection traces - System caches - Windows Search databases - Volume Shadow Copy	- Windows 7 artifacts - 64 bits Windows
File System Forensics	- FAT, NTFS, UDF - Metadata (NTFS MFT, FAT Directory entry) - Timestamps - Transaction logs (NTFS)	
Web Browser Forensics	- History, Cache, Cookie - Internet usage history (URLs, Search Keywords…)	- MS Internet Explorer - Google Chrome
E-mail Forensics	- MS Outlook file examination - E-mails and attachments	
Database Forensics	- MS Extensible Storage Engine (ESE) Database - SQLite Database	- Windows Search - MS Internet Explorer - Google Chrome - Google Drive
Deleted Data Recovery	- Metadata based recovery - Signature & Content based recovery (aka Carving) - Recycle Bin of Windows - Unused area examination	
User Behavior Analysis	- Constructing a forensic timeline of events - Visualizing the timeline	

6. QUESTIONS AND ANSWERS ABOUT THE SCENARIO

1) What are the hash values (MD5 & SHA-1) of all images?

Does the acquisition and verification hash value match?

Possible Answer	Class	Hash Algo.	Hash value
	PC	MD5	A49D1254C873808C58E6F1BCD60B5BDE
		SHA-1	AFE5C9AB487BD47A8A9856B1371C2384D44FD785
	RM#2	MD5	B4644902ACAB4583A1D0F9F1A08FAA77
		SHA-1	048961A85CA3ECED8CC73F1517442D31D4DCA0A3
	RM#3 (Type1)	MD5	858C7250183A44DD83EB706F3F178990
		SHA-1	471D3EEDCA9ADD872FC0708297284E1960FF44F8
	RM#3 (Type2)	MD5	858C7250183A44DD83EB706F3F178990
		SHA-1	471D3EEDCA9ADD872FC0708297284E1960FF44F8
	RM#3 (Type3)	MD5	DF914108FB3D86744EB688EBA482FBDF
		SHA-1	7F3C2EB1F1E2DB97BE6E963625402A0E362A532C
Considerations	N/A		

2) Identify the partition information of PC image.

Possible Answer	No.	Bootable	File system	Start Sector	Total Sectors	Size
	1		NTFS	2,048	204,800	100 MB
	2	*	NTFS	206,848	41,734,144	19.9 GB
Considerations	N/A					

3) Explain installed OS information in detail.

(OS name, install date, registered owner…)

Possible Answer	OS Name	Windows 7 Ultimate
	Version	6.1
	Build Number	7601
	Registered Owner	informant
	System Root	C:\\Windows
	Install Date	2015-03-22 14:34:26 (GMT)
Considerations	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion	

4) What is the timezone setting?

Possible Answer	Timezone	Eastern Time (US & Canada) (UTC-05:00)
	Daylight Time Bias	+1
Considerations	HKLM\SYSTEM\ControlSet###\Control\TimeZoneInformation	

5) What is the computer name?

Possible Answer	INFORMANT-PC
Considerations	HKLM\SYSTEM\ControlSet###\Control\ComputerName\ComputerName (value: ComputerName) HKLM\SYSTEM\ControlSet###\Services\Tcpip\Parameters (value: Hostname) ……

6) List all accounts in OS except the system accounts: *Administrator, Guest, systemprofile*, *LocalService*, *NetworkService*. (Account name, login count, last logon date…)

Possible Answer (Timezone is applied)	Account	SID	NT Hash	Status	Login Count	Account Created Time	Last Login Time	Login Failure Time
	informant	1000	(a)	Enabled	10	2015-03-22 09:33:54	2015-03-25 09:45:59	2015-03-25 09:45:43
	admin11	1001	(b)	Enabled	2	2015-03-22 10:51:54	2015-03-22 10:57:02	2015-03-22 10:53:02
	ITechTeam	1002	(c)	Enabled	0	2015-03-22 10:52:30	-	-
	Temporary	1003	(d)	Enabled	1	2015-03-22 10:53:01	2015-03-22 10:55:57	2015-03-22 10:56:37
Considerations	- HKLM\SAM\~ - SYSTEM hive is required for calculating hash values of passwords. - NT Hashes and user passwords (it will be useful for practicing Windows password cracking) (a) 9E3D31B073E60BFD7B07978D6F914D0A → Password: *informant#suspect1* (b) 21759544B2D7EFCCC978449463CF7E63 → Password: *djemals11* (c) 75ED0CB7676889AB43764A3B7D3E6943 → Password: *dkdlxpzmxla* (d) 1B3801B608A6BE89D21FD3C5729D30BF → Password: *xpavhfkfl*							

7) Who was the last user to logon into PC?

Possible Answer	informant
Considerations	HKLM\SAM\~

8) When was the last recorded shutdown date/time?

Possible Answer	2015-03-25 11:31:05 (Eastern Time + DST)
Considerations	HKLM\SYSTEM\ControlSet###\Control\Windows (value: ShutdownTime)

9) Explain the information of network interface(s) with an IP address assigned by DHCP.

Possible Answer	Device Name	Intel(R) PRO/1000 MT Network Connection
	IP Address	10.11.11.129
	Subnet Mask	255.255.255.0
	Name Server	10.11.11.2
	Domain	localdomain
	Default Gateway	10.11.11.2
	DHCP Usage	Yes
	DHCP Server	10.11.11.254
Considerations	HKLM\SYSTEM\ControlSet###\Services\Tcpip\Parameters\Interfaces\{GUID}	

10) What applications were installed by the suspect after installing OS?

Possible Answer (Timezone is applied)	Installation Time	Name	Version	Manufacturer	Installation Path
	2015-03-22 10:04:14	Microsoft Office Professional Plus 2013	15.0.4420.1017	Microsoft Corporation	C:\Program Files\Microsoft Office
	2015-03-22 10:11:51	Google Chrome	41.0.2272.101	Google Inc.	C:\Program Files (x86)\Google\Chrome\Application

	2015-03-22 10:16:03	Google Update Helper	1.3.26.9	Google Inc.	
	2015-03-23 15:00:45	Apple Application Support	3.0.6	Apple Inc.	C:\Program Files (x86)\Common Files\Apple\Apple Application Support\
	2015-03-23 15:00:58	Bonjour	3.0.0.10	Apple Inc.	C:\Program Files (x86)\Bonjour\
	2015-03-23 15:01:01	Apple Software Update	2.1.3.127	Apple Inc.	C:\Program Files (x86)\Apple Software Update\
	2015-03-23 15:02:46	Google Drive	1.20.8672.3137	Google Inc.	
	2015-03-25 09:51:39	Microsoft .NET Framework 4	4.0.30319	Microsoft Corporation	C:\Windows\Microsoft.NET\Framework64\v4.0.30319
	2015-03-25 09:57:31	Eraser	6.2.2962	The Eraser Project	
Considerations	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\~ HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\~ …				

11) List application execution logs.

(Executable path, execution time, execution count...)

	Timestamp	Execution Path	Count	Source
Possible Answer	2015-03-22 11:11:04	C:\Users\informant\Desktop\temp\IE11-Windows6.1-x64-en-us.exe	N/A	Shimcache
(Some Windows executables and duplicated items are excluded)	2015-03-22 11:11:04	C:\Users\informant\Desktop\Download\IE11-Windows6.1-x64-en-us.exe	N/A	Shimcache
	2015-03-22 11:12:32	C:\Users\informant\Desktop\Download\IE11-Windows6.1-x64-en-us.exe	1	UserAssist
	2015-03-23 15:56:33	C:\Users\informant\Downloads\googledrivesync.exe	N/A	Shimcache
	2015-03-23 15:56:33	C:\Users\INFORM~1\AppData\Local\Temp\GUMA150.tmp\GoogleUpdateSetup.exe	N/A	Shimcache
	2015-03-23 15:56:33	C:\Users\informant\Downloads\icloudsetup.exe	N/A	Shimcache
(Timezone is applied)	2015-03-23 16:00:59	C:\Windows\Installer\{789A5B64-9DD9-4BA5-915A-F0FC0A1B7BFE}\AppleSoftwareUpdateIco.exe	N/A	Shimcache
	2015-03-23 16:02:07	C:\Users\INFORM~1\AppData\Local\Temp\GUMA150.tmp\GoogleUpdate.exe	N/A	Shimcache
	2015-03-23 16:02:09	C:\Program Files (x86)\GUMA94B.tmp\GoogleUpdate.exe	N/A	Shimcache
	2015-03-23 16:26:50	C:\PROGRAM FILES\Microsoft Office\Office15\EXCEL.EXE	1	UserAssist
	2015-03-23 16:27:33	C:\PROGRAM FILES\Microsoft Office\Office15\POWERPNT.EXE	2	UserAssist
	2015-03-24 14:29:07	C:\PROGRAM FILES\MICROSOFT GAMES\SOLITAIRE\SOLITAIRE.EXE	1	Prefetch
	2015-03-24 14:31:55	C:\Windows\System32\StikyNot.exe	2	Prefetch
	2015-03-24 14:31:55	Microsoft.Windows.StickyNotes	13	UserAssist
	2015-03-24 17:05:38	C:\PROGRAM FILES (X86)\GOOGLE\CHROME\APPLICATION\CHROME.EXE	71	Prefetch
	2015-03-25 10:41:03	C:\PROGRAM FILES\MICROSOFT OFFICE\OFFICE15\OUTLOOK.EXE	1	Prefetch
	2015-03-25 10:41:03	C:\PROGRAM FILES\MICROSOFT OFFICE\OFFICE15\OUTLOOK.EXE	5	UserAssist

	2015-03-25 10:42:47	C:\PROGRAM FILES (X86)\WINDOWS MEDIA PLAYER\wmplayer.exe	1	Prefetch
	2015-03-25 10:42:47	Microsoft.Windows.MediaPlayer32	1	UserAssist
	2015-03-25 10:47:40	C:\Users\informant\Desktop\Download\Eraser 6.2.0.2962.exe	N/A	Shimcache
	2015-03-25 10:48:28	C:\Users\informant\Desktop\Download\ccsetup504.exe	N/A	Shimcache
	2015-03-25 10:50:14	C:\USERS\INFORMANT\DESKTOP\DOWNLOAD\ERASER 6.2.0.2962.EXE	1	Prefetch
	2015-03-25 10:50:14	C:\USERS\INFORMANT\DESKTOP\DOWNLOAD\ERASER 6.2.0.2962.EXE	1	UserAssist
	2015-03-25 10:50:15	C:\Users\INFORM~1\AppData\Local\Temp\eraserInstallBootstrapper\dotNetFx40_Full_setup.exe	N/A	Shimcache
	2015-03-25 10:50:15	C:\USERS\INFORMANT\APPDATA\LOCAL\TEMP\ERASERINSTALLBOOTSTRAPPER\DOTNETFX40_FULL_SETUP.EXE	1	Prefetch
	2015-03-25 10:57:56	C:\USERS\INFORMANT\DESKTOP\DOWNLOAD\CCSETUP504.EXE	1	Prefetch
	2015-03-25 10:57:56	C:\USERS\INFORMANT\DESKTOP\DOWNLOAD\CCSETUP504.EXE	1	UserAssist
	2015-03-25 11:12:28	C:\PROGRAM FILES\Eraser\Eraser.exe	1	UserAssist
	2015-03-25 11:13:30	C:\PROGRAM FILES\Eraser\Eraser.exe	2	Prefetch
	2015-03-25 11:15:50	C:\PROGRAM FILES\CCLEANER\CCLEANER64.EXE	1	UserAssist
	2015-03-25 11:15:50	C:\PROGRAM FILES\CCLEANER\CCLEANER64.EXE	2	Prefetch
	2015-03-25 11:16:00	C:\PROGRAM FILES (X86)\GOOGLE\UPDATE\GOOGLEUPDATE.EXE	38	Prefetch
	2015-03-25 11:18:29	C:\PROGRAM FILES\CCLEANER\UNINST.EXE	1	Prefetch
	2015-03-25 11:21:30	C:\PROGRAM FILES (X86)\GOOGLE\DRIVE\GOOGLEDRIVESYNC.EXE	1	UserAssist
	2015-03-25 11:21:31	C:\PROGRAM FILES (X86)\GOOGLE\DRIVE\GOOGLEDRIVESYNC.EXE	2	Prefetch
	2015-03-25 11:22:06	C:\PROGRAM FILES\INTERNET EXPLORER\iexplore.exe	2	Prefetch
	2015-03-25 11:22:07	C:\PROGRAM FILES (X86)\INTERNET EXPLORER\iexplore.exe	14	Prefetch
	2015-03-25 11:24:48	C:\PROGRAM FILES\MICROSOFT OFFICE\OFFICE15\WINWORD.EXE	3	Prefetch
	2015-03-25 11:24:48	C:\PROGRAM FILES\MICROSOFT OFFICE\OFFICE15\WINWORD.EXE	4	UserAssist
	2015-03-25 11:28:47	C:\Windows\System32\xpsrchvw.exe	1	Prefetch
	2015-03-25 11:28:47	C:\Windows\System32\xpsrchvw.exe	1	UserAssist
	N/A	C:\Users\informant\Downloads\icloudsetup.exe	N/A	UserAssist
	N/A	C:\PROGRAM FILES (X86)\Common Files\Apple\Internet Services\iCloud.exe	N/A	UserAssist
	N/A	C:\Users\informant\AppData\Local\Temp\eraserInstallBootstrapper\dotNetFx40_Full_setup.exe	N/A	UserAssist
	MuiCache	C:\Program Files\Internet Explorer\iexplorer.exe		
	MuiCache	C:\Users\informant\Desktop\Download\IE11-Windows6.1-x64-en-us.exe		
	MuiCache	C:\Windows\System32\xpsrchvw.exe (XPS Viewer)		
Considerations	* 'Execution Count' may not be accurate. * Timestamps of UserAssist and Prefetch: 'Execution Time' * Timestamps of Shimcache: 'Last Modified Time' from filesystem metadata			

<table>
<tr><td rowspan="7"></td><td colspan="2">[File] Windows Prefetch folder</td></tr>
</table>

[File] Windows Prefetch folder > \Windows\Prefetch*.pf > Executable file paths and their execution timestamps (+ execution counts) [File] IconCache > \Users\informant\AppData\Local\IconCache.db > Executable file paths and their icon images [Reg] UserAssist > HKU\informant\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist*\Count\ > Executable file paths and their execution timestamps (+ execution counts) [Reg] Application Compatibility (Shimcache) > HKLM\SYSTEM\ControlSet###\Control\Session Manager\AppCompatCache\ > Executable file paths and their modified timestamps [Reg] Application Compatibility Cache > HKU\informant\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\ > Executable file paths and their modified timestamps [Reg] MuiCache > HKU\informant\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache\ > Executable file paths

12) List all traces about the system on/off and the user logon/logoff.

(It should be considered only during a time range between 09:00 and 18:00 in the timezone from Question 4.)

	Time Generated	Event ID	Description
Possible Answer (Some duplicated and meaningless items are excluded) (Timezone is applied)	2015-03-22 10:51:14	4608	Starting up
	2015-03-22 11:00:08	4624	Logon
	2015-03-22 11:22:54	4624	Logon
	2015-03-22 12:00:08	4647	Logoff
	2015-03-22 12:00:09	1100	Shutdown
	2015-03-23 13:24:23	4624	Logon
	2015-03-23 13:24:23	4608	Starting up
	2015-03-23 14:36:07	4624	Logon
	2015-03-23 16:00:22	4624	Logon
	2015-03-23 16:01:02	4624	Logon
	2015-03-23 17:02:53	4647	Logoff
	2015-03-23 17:02:59	1100	Shutdown
	2015-03-24 09:21:29	4624	Logon
	2015-03-24 09:21:29	4608	Starting up
	2015-03-24 09:23:40	4624	Logon
	2015-03-24 11:14:30	4624	Logon
	2015-03-24 11:22:39	4624	Logon
	2015-03-24 11:46:14	4624	Logon
	2015-03-24 14:28:38	4624	Logon
	2015-03-24 16:58:52	4624	Logon
	2015-03-24 17:07:25	4647	Logoff
	2015-03-24 17:07:26	1100	Shutdown
	2015-03-25 09:05:41	4624	Logon
	2015-03-25 09:05:41	4608	Starting up
	2015-03-25 09:07:49	4624	Logon
	2015-03-25 09:23:59	4624	Logon
	2015-03-25 10:31:53	4624	Logon

2015-03-25 10:45:59	4637	Logoff
2015-03-25 10:50:28	4624	Logon
2015-03-25 10:50:30	4624	Logon
2015-03-25 10:50:50	4624	Logon
2015-03-25 10:56:55	4624	Logon
2015-03-25 10:57:18	4624	Logon
2015-03-25 11:18:54	4624	Logon
2015-03-25 11:30:57	4647	Logoff
2015-03-25 11:31:00	1100	Shutdown

Considerations	- Security event logs
	- Event IDs for Windows Vista or higher
	  : 4608 (Windows is starting up), 1100 (service shutdown)
	  : 4624 (successful logon), 4634 (logoff), 4625 (logon failure), 4647 (a user initiated the logoff process)...
	* Some events may not be accurate.

13) What web browsers were used?

Possible Answer	- Microsoft Internet Explorer v11.0.9600.17691 (Microsoft Internet Explorer 9 or lower → updated to IE 11 version) - Google Chrome v41.0.2272.101
Considerations	HKLM\SOFTWARE\Microsoft\Internet Explorer (value: svcVersion) HKU\informant\Software\Google\Chrome\BLBeacon (value: version)

14) Identify directory/file paths related to the web browser history.

Possible Answer	MS IE (9 or lower)	C:\Users\informant\AppData\Local\Microsoft\Windows\History\ C:\Users\informant\AppData\Local\Microsoft\Windows\Temporary Internet Files\ C:\Users\informant\AppData\Roaming\Microsoft\Windows\Cookies\
	MS IE 11	C:\Users\informant\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat
	Chrome	C:\Users\informant\AppData\Local\Google\Chrome\User Data\Default\History C:\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Application Cache\ C:\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Media Cache\ C:\Users\informant\AppData\Local\Google\Chrome\User Data\Default\GPUCache\ C:\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Cookies\ C:\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies\ C:\Users\informant\AppData\Local\Google\Chrome\User Data\Default\Extensions\ ……
Considerations		- History, Cache, Cookie… - Windows Search database (related to Question 42 ~ 46) > C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb

15) What websites were the suspect accessing? (Timestamp, URL...)

Possible Answer	Timestamp	URL	Browser
	2015-03-22 11:09:01	http://windows.microsoft.com/en-us/internet-explorer/ie-8-welcome	IE 8
	2015-03-22 11:09:47	https://www.google.com/	IE 8
(Some duplicated and meaningless items are excluded)	2015-03-22 11:10:50	http://windows.microsoft.com/en-us/internet-explorer/download-ie	IE 8
	2015-03-22 11:11:04	http://download.microsoft.com/download/7/1/7/7179A150-F2D2-4502-9D70-4B59EA148EAA/IE11-Windows6.1-x64-en-us.exe	IE 8
	2015-03-22 11:11:06	https://dl.google.com/update2/1.3.26.9/GoogleInstaller_en.application?appguid%3D%7B8A69D345-D564-463C-AFF1-	IE 8
	2015-03-22 11:11:58	https://www.google.com/intl/en/chrome/browser/welcome.html	Chrome
	2015-03-22 11:27:59	https://www.google.com/#q=outlook+2013+settings	Chrome

(Timezone is applied)	2015-03-23 13:26:58	http://www.bing.com/	Chrome
	2015-03-23 13:26:58	https://www.google.com/webhp?hl=en	Chrome
	2015-03-23 13:27:36	http://go.microsoft.com/fwlink/?LinkId=69157	IE 11
	2015-03-23 13:27:49	http://www.microsoft.com/en-us/ie-firstrun/win-7/ie-11/vie	IE 11
	2015-03-23 14:02:09	https://www.google.com/webhp?hl=en#hl=en&q=data+leakage+methods	Chrome
	2015-03-23 14:02:18	http://www.sans.org/reading-room/whitepapers/awareness/data-leakage-threats-mitigation_1931	Chrome
	2015-03-23 14:02:44	https://www.google.com/webhp?hl=en#hl=en&q=leaking+confidential+information	Chrome
	2015-03-23 14:03:40	https://www.google.com/webhp?hl=en#hl=en&q=information+leakage+cases	Chrome
	2015-03-23 14:04:54	http://www.emirates247.com/business/technology/top-5-sources-leaking-personal-data-2015-03-	Chrome
	2015-03-23 14:05:48	https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=intellectual+property+theft	Chrome
	2015-03-23 14:05:55	http://www.fbi.gov/about-us/investigate/white_collar/ipr/ipr	Chrome
	2015-03-23 14:06:01	http://en.wikipedia.org/wiki/Intellectual_property	Chrome
	2015-03-23 14:06:27	https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=how+to+leak+a+secret	Chrome
	2015-03-23 14:06:53	http://research.microsoft.com/en-us/um/people/yael/publications/2001-leak_secret.pdf	Chrome
	2015-03-23 14:07:58	http://www.bing.com/news/search?q=file+sharing+and+tethering&FORM=HDRSC6	IE 11
	2015-03-23 14:08:18	http://sysinfotools.com/blog/tethering-internet-files-sharing/	IE 11
	2015-03-23 14:08:31	http://www.bing.com/search?q=DLP%20DRM&qs=n&form=QBRE&pq=dlp%20drm&sc=8-7&sp=-1&sk=&cvid=6e206ee8751e4ad89f882ed52daf3aea&sid=BE5E388F8757406CAA32E58334719A20&format=jsonv2&jsoncbid=0	IE 11
	2015-03-23 14:08:54	http://www.bing.com/search?q=e-mail%20investigation&qs=n&form=QBRE&pq=e-mail%20investigation&sc=8-7&sp=-1&sk=&cvid=fe1c3738d8c7471284731724166959af&sid=BE5E388F8757406CAA32E58334719A20&format=jsonv2&jsoncbid=1	IE 11
	2015-03-23 14:10:03	http://www.bing.com/search?q=Forensic+Email+Investigation&FORM=QSRE1&sid=BE5E388F8757406CAA32E58334719A20&format=jsonv2&jsoncbid=3	IE 11
	2015-03-23 14:10:27	http://www.bing.com/search?q=what%20is%20windows%20system%20artifacts&qs=n&form=QBRE&pq=what%20is%20windows%20system%20artifacts&sc=0-27&sp=-1&sk=&cvid=1ef4ace146854d97acf263b53bf97b8c&sid=BE5E388F8757406CAA32E58334719A20&format=jsonv2&jsoncbid=4	IE 11
	2015-03-23 14:11:12	http://resources.infosecinstitute.com/windows-systems-and-artifacts-in-digital-forensics-part-i-registry/	IE 11
	2015-03-23 14:11:50	http://www.bing.com/search?q=investigation%20on%20windows%20machine&qs=n&form=QBRE&pq=investigation%20on%20windows%20machine&sc=8-4&sp=-1&sk=&cvid=eb73de7f523c48769d56201379f55e67&sid=BE5E388F8757406CAA32E58334719A20&format=jsonv2&jsoncbid=5	IE 11
	2015-03-23 14:12:07	https://technet.microsoft.com/en-us/library/cc162846.aspx	IE 11
	2015-03-23 14:12:35	http://www.bing.com/search?q=windows%20event%20logs&qs=n&form=QBRE&pq=windows%20event%20logs&sc=0-32&sp=-1&sk=&cvid=36b33ac5151246398f7dc1ca79de069c&sid=BE5E388F8757406CAA32E58334719A20&format=jsonv2&jsoncbid=6	IE 11
	2015-03-23 14:12:45	https://support.microsoft.com/en-us/kb/308427	IE 11

2015-03-23 14:12:52	http://en.wikipedia.org/wiki/Event_Viewer	IE 11
2015-03-23 14:13:20	http://www.bing.com/search?q=cd%20burning%20method&qs=n&form=Q BRE&pq=cd%20burning%20method&sc=8-2&sp=- 1&sk=&cvid=b7dbe6fb67424c578172ba57330a0894&sid=BE5E388F8757 406CAA32E58334719A20&format=jsonv2&jsoncbid=7	IE 11
2015-03-23 14:13:37	http://www.bing.com/search?q=cd%20burning%20method%20in%20windo ws&qs=n&form=QBRE&pq=cd%20burning%20method%20in%20window s&sc=0-0&sp=- 1&sk=&cvid=acec9b1dcb8146c58258ad65c770d76e&sid=BE5E388F87574 06CAA32E58334719A20&format=jsonv2&jsoncbid=8	IE 11
2015-03-23 14:13:57	https://msdn.microsoft.com/en- us/library/windows/desktop/dd562212(v=vs.85).aspx	IE 11
2015-03-23 14:14:11	http://www.bing.com/search?q=external%20device%20and%20forensics&q s=n&form=QBRE&pq=external%20device%20and%20forensics&sc=8- 9&sp=- 1&sk=&cvid=c30c4b1f36114b1c9bc683838c69823a&sid=BE5E388F87574 06CAA32E58334719A20&format=jsonv2&jsoncbid=9	IE 11
2015-03-23 14:14:24	http://www.forensicswiki.org/wiki/USB_History_Viewing	IE 11
2015-03-23 14:14:50	https://www.google.com/search?q=information+leakage+cases&hl=en&biw =950&bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVY H3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=cloud+s torage	Chrome
2015-03-23 14:15:09	http://en.wikipedia.org/wiki/Cloud_storage	Chrome
2015-03-23 14:15:32	http://www.pcadvisor.co.uk/test-centre/internet/3506734/best-cloud-storage- dropbox-google-drive-onedrive-icloud/	Chrome
2015-03-23 14:15:44	https://www.google.com/search?q=information+leakage+cases&hl=en&biw =950&bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVY H3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=digital+ forensics	Chrome
2015-03-23 14:15:49	http://en.wikipedia.org/wiki/Digital_forensics	Chrome
2015-03-23 14:16:06	http://nij.gov/topics/forensics/evidence/digital/pages/welcome.aspx	Chrome
2015-03-23 14:16:55	https://www.google.com/search?q=information+leakage+cases&hl=en&biw =950&bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVY H3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=how+to +delete+data	Chrome
2015-03-23 14:17:14	https://www.google.com/search?q=information+leakage+cases&hl=en&biw =950&bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVY H3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=anti- forensics	Chrome
2015-03-23 14:17:19	http://forensicswiki.org/wiki/Anti-forensic_techniques	Chrome
2015-03-23 14:18:00	https://defcon.org/images/defcon-20/dc-20-presentations/Perklin/DEFCON- 20-Perklin-AntiForensics.pdf	Chrome
2015-03-23 14:18:10	https://www.google.com/search?q=information+leakage+cases&hl=en&biw =950&bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVY H3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=system +cleaner	Chrome
2015-03-23 14:18:30	https://www.google.com/search?q=information+leakage+cases&hl=en&biw =950&bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVY H3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=how+to +recover+data	Chrome
2015-03-23 14:19:03	https://www.google.com/search?q=information+leakage+cases&hl=en&biw =950&bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVY H3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=data+re covery+tools	Chrome
2015-03-23 14:19:17	http://en.wikipedia.org/wiki/List_of_data_recovery_software	Chrome
2015-03-23 14:19:21	http://www.forensicswiki.org/wiki/Tools:Data_Recovery	Chrome
2015-03-23 15:55:09	https://www.google.com/webhp?hl=en#hl=en&q=apple+icloud	Chrome
2015-03-23 15:55:28	https://www.apple.com/icloud/setup/pc.html	Chrome

	2015-03-23 15:56:04	https://www.google.com/webhp?hl=en#hl=en&q=google+drive	Chrome
	2015-03-23 15:56:15	https://www.google.com/drive/download/	Chrome
	2015-03-23 16:43:52	http://www.bing.com/news?FORM=Z9LH3	IE 11
	2015-03-23 16:45:30	http://www.bing.com/news?q=Soccer+News&FORM=NSBABR	IE 11
	2015-03-23 16:53:46	http://www.bing.com/news?q=top+stories&FORM=NWRFSH	IE 11
	2015-03-23 16:55:10	http://www.bing.com/news?q=world+news&FORM=NSBABR	IE 11
	2015-03-23 16:55:18	http://www.bing.com/news?q=entertainment+news&FORM=NSBABR	IE 11
	2015-03-23 16:55:54	http://www.bing.com/news?q=business+news&FORM=NSBABR	IE 11
	2015-03-24 11:22:46	https://news.google.com/news/section?pz=1&cf=all&ned=us&topic=w&siidp=0b2226a6a5dab3b27ee85fc5e8d21f28f01e	Chrome
	2015-03-24 11:23:16	https://news.google.com/news/section?pz=1&cf=all&ned=us&topic=tc&siidp=e6116f8175cb189b8dd7fd58ef6bc922ec04&ar=1427212899	Chrome
	2015-03-24 14:59:52	https://news.google.com/news?pz=1&cf=all&ned=us&siidp=0c33ef04190b3734a22c5bae18801ff1041e	Chrome
	2015-03-24 15:00:27	https://news.google.com/news/section?pz=1&cf=all&ned=us&topic=w&siidp=538c61c825aba06be7485be747a619778015	Chrome
	2015-03-24 17:06:50	https://www.google.com/#q=security+checkpoint+cd-r	Chrome
	2015-03-25 10:46:44	http://www.bing.com/search?q=anti-forensic+tools&qs=n&form=QBLH&pq=anti-forensic+tools&sc=8-13&sp=-1&sk=&cvid=e799e715fa2244a5a7967675bdcca9d3	IE 11
	2015-03-25 10:46:54	http://www.bing.com/search?q=eraser&qs=n&form=QBRE&pq=eraser&sc=8-6&sp=-1&sk=&cvid=e3b983fe889944179093ff5199b2eac4&sid=C7E8F3776E804120B57C623F21EF33C4&format=jsonv2&jsoncbid=0	IE 11
	2015-03-25 10:46:59	http://eraser.heidi.ie/	IE 11
	2015-03-25 10:47:34	http://iweb.dl.sourceforge.net/project/eraser/Eraser%206/6.2/Eraser%206.2.0.2962.exe	IE 11
	2015-03-25 10:47:51	http://www.bing.com/search?q=ccleaner&qs=n&form=QBRE&pq=ccleaner&sc=8-8&sp=-1&sk=&cvid=d434736d4e514ad497f68734a6779104&sid=C7E8F3776E804120B57C623F21EF33C4&format=jsonv2&jsoncbid=1	IE 11
	2015-03-25 10:48:12	http://www.piriform.com/ccleaner/download	IE 11
Considerations	- History, Cache, Cookie…		

16) List all search keywords using web browsers. (Timestamp, URL, keyword...)

Possible Answer	Timestamp	Keyword (URL)	Browser
(Some duplicated and meaningless items are excluded) (Timezone is applied)	2015-03-23 14:02:09	**data leakage method** (https://www.google.com/webhp?hl=en#hl=en&q=**data+leakage+methods**)	Chrome
	2015-03-23 14:02:44	**leaking confidential information** (https://www.google.com/webhp?hl=en#hl=en&q=**leaking+confidential+information**)	Chrome
	2015-03-23 14:03:40	**information leakage cases** (https://www.google.com/webhp?hl=en#hl=en&q=**information+leakage+cases**)	Chrome
	2015-03-23 14:05:48	**intellectual property theft** (https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950&bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1sQTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=**intellectual+property+theft**)	Chrome
	2015-03-23 14:06:27	**how to leak a secret**	Chrome

		(https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950 &bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1s QTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=**how+to+leak+a+secret**)	
2015-03-23 14:07:58	**file sharing and tethering** (http://www.bing.com/news/search?q=**file+sharing+and+tethering**&FORM =HDRSC6)		IE 11
2015-03-23 14:08:31	**DLP DRM** (http://www.bing.com/search?q=**DLP%20DRM**&qs=n&form=QBRE&pq=**d lp%20drm**&sc=8-7&sp=- 1&sk=&cvid=6e206ee8751e4ad89f882ed52daf3aea&sid=BE5E388F87574 06CAA32E58334719A20&format=jsonv2&jsoncbid=0)		IE 11
2015-03-23 14:08:54	**e-mail investigation** (http://www.bing.com/search?q=**e- mail%20investigation**&qs=n&form=QBRE&pq=**e- mail%20investigation**&sc=8-7&sp=- 1&sk=&cvid=fe1c3738d8c7471284731724166959af&sid=BE5E388F875740 6CAA32E58334719A20&format=jsonv2&jsoncbid=1)		IE 11
2015-03-23 14:10:03	**Forensic Email Investigation** (http://www.bing.com/search?q=**Forensic+Email+Investigation**&FORM=QSRE1 &sid=BE5E388F8757406CAA32E58334719A20&format=jsonv2&jsoncbid=3)		IE 11
2015-03-23 14:10:27	**what is windows system artifacts** (http://www.bing.com/search?q=**what%20is%20windows%20system%20a rtifacts**&qs=n&form=QBRE&pq=**what%20is%20windows%20system%2 0artifacts**&sc=0-27&sp=- 1&sk=&cvid=1ef4ace146854d97acf263b53bf97b8c&sid=BE5E388F8757406 CAA32E58334719A20&format=jsonv2&jsoncbid=4)		IE 11
2015-03-23 14:11:50	**investigation on windows machine** (http://www.bing.com/search?q=**investigation%20on%20windows%20mac hine**&qs=n&form=QBRE&pq=**investigation%20on%20windows%20mac hine**&sc=8-4&sp=- 1&sk=&cvid=eb73de7f523c48769d56201379f55e67&sid=BE5E388F875740 6CAA32E58334719A20&format=jsonv2&jsoncbid=5)		IE 11
2015-03-23 14:12:35	**windows event logs** (http://www.bing.com/search?q=**windows%20event%20logs**&qs=n&form= QBRE&pq=**windows%20event%20logs**&sc=0-32&sp=- 1&sk=&cvid=36b33ac5151246398f7dc1ca79de069c&sid=BE5E388F875740 6CAA32E58334719A20&format=jsonv2&jsoncbid=6)		IE 11
2015-03-23 14:13:20	**cd burning method** (http://www.bing.com/search?q=**cd%20burning%20method**&qs=n&form= QBRE&pq=**cd%20burning%20method**&sc=8-2&sp=- 1&sk=&cvid=b7dbe6fb67424c578172ba57330a0894&sid=BE5E388F875740 6CAA32E58334719A20&format=jsonv2&jsoncbid=7)		IE 11
2015-03-23 14:13:37	**cd burning method in windows** (http://www.bing.com/search?q=**cd%20burning%20method%20in%20win dows**&qs=n&form=QBRE&pq=**cd%20burning%20method%20in%20win dows**&sc=0-0&sp=- 1&sk=&cvid=acec9b1dcb8146c58258ad65c770d76e&sid=BE5E388F875740 6CAA32E58334719A20&format=jsonv2&jsoncbid=8)		IE 11
2015-03-23 14:14:11	**external device and forensics** (http://www.bing.com/search?q=**external%20device%20and%20forensics** &qs=n&form=QBRE&pq=**external%20device%20and%20forensics**&sc=8 -9&sp=- 1&sk=&cvid=c30c4b1f36114b1c9bc683838c69823a&sid=BE5E388F875740 6CAA32E58334719A20&format=jsonv2&jsoncbid=9)		IE 11
2015-03-23 14:14:50	**cloud storage** (https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950 &bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1s QTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=**cloud+storage**)		Chrome

	2015-03-23 14:15:44	**digital forensics** (https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950 &bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1s QTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=**digital+forensics**)	Chrome
	2015-03-23 14:16:55	**how to delete data** (https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950 &bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1s QTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=**how+to+delete+data**)	Chrome
	2015-03-23 14:17:14	**anti-forensics** (https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950 &bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1s QTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=**anti-forensics**)	Chrome
	2015-03-23 14:18:10	**system cleaner** (https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950 &bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1s QTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=**system+cleaner**)	Chrome
	2015-03-23 14:18:30	**how to recover data** (https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950 &bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1s QTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=**how+to+recover+data**)	Chrome
	2015-03-23 14:19:03	**data recovery tools** (https://www.google.com/search?q=information+leakage+cases&hl=en&biw=950 &bih=499&site=webhp&tbm=vid&source=lnms&sa=X&ei=3VUQVYH3FMO1s QTf1YGwBw&ved=0CAoQ_AUoBA&dpr=1#hl=en&q=**data+recovery+tools**)	Chrome
	2015-03-23 15:55:09	**apple icloud** (https://www.google.com/webhp?hl=en#hl=en&q=**apple+icloud**)	Chrome
	2015-03-23 15:56:04	**google drive** (https://www.google.com/webhp?hl=en#hl=en&q=**google+drive**)	Chrome
	2015-03-24 17:06:50	**security checkpoint cd-r** (https://www.google.com/#q=**security+checkpoint+cd-r**)	Chrome
	2015-03-25 10:46:44	**anti-forensic tools** (http://www.bing.com/search?q=**anti-forensic+tools**&qs=n&form=QBLH&pq=**anti-forensic+tools**&sc=8-13&sp=-1&sk=&cvid=e799e715fa2244a5a7967675bdcca9d3)	IE 11
	2015-03-25 10:46:54	**eraser** (http://www.bing.com/search?q=**eraser**&qs=n&form=QBRE&pq=**eraser**&sc=8-6&sp=-1&sk=&cvid=e3b983fe889944179093ff5199b2eac4&sid=C7E8F3776E804120B57C623F21EF33C4&format=jsonv2&jsoncbid=0)	IE 11
	2015-03-25 10:47:51	**ccleaner** (http://www.bing.com/search?q=**ccleaner**&qs=n&form=QBRE&pq=**ccleaner**&sc=8-8&sp=-1&sk=&cvid=d434736d4e514ad497f68734a6779104&sid=C7E8F3776E804120B57C623F21EF33C4&format=jsonv2&jsoncbid=1)	IE 11
Considerations	- Web browser logs		

17) List all user keywords at the search bar in Windows Explorer. (Timestamp, Keyword)

Possible Answer	Timestamp (Timezone is applied)	Search Keyword
	2015-03-23 14:40:17	secret
Considerations	HKU\informant\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery\ - 'Timestamp' can be inferred from a timestamp of the parent key ('WordWheelQuery'). - 'Timestamp' may not be accurate because it depends on the update mechanism of Windows Explorer.	

18) What application was used for e-mail communication?

Possible Answer	Microsoft Outlook 2013
Considerations	HKLM\SOFTWARE\Classes\mailto\shell\open\command (→Microsoft Outlook) HKLM\SOFTWARE\Clients\Mail (→Microsoft Outlook) HKU\informant\Software\Microsoft\Office\15.0\Outlook …

19) Where is the e-mail file located?

Possible Answer	C:\Users\informant\AppData\Local\Microsoft\Office\iaman.informant@nist.gov.ost
Considerations	- Microsoft Outlook 2013 - Microsoft OST file format HKEY_USERS\informant\Software\Microsoft\Office\15.0\Outlook\Search (value: C:\Users\informant\AppData\Local\Microsoft\Outlook\iaman.informant@nist.gov.ost) HKEY_USERS\informant\Software\Microsoft\Office\15.0\Outlook\PST (value: LastCorruptStore)

20) What was the e-mail account used by the suspect?

Possible Answer	iaman.informant@nist.gov
Considerations	- See Question 19.

21) List all e-mails of the suspect. If possible, identify deleted e-mails.

(You can identify the following items: *Timestamp*, *From*, *To*, *Subject*, *Body*, and *Attachment*)

[Hint: just examine the OST file only.]

Possible Answer (Timezone is applied)	Timestamp	E-Mail Communication	
	2015-03-23 13:29:27	Source	[Inbox]
		From → To	spy.conspirator@nist.gov → iaman.informant@nist.gov
		Subject	Hello, Iaman
		Body	How are you doing?
	2015-03-23 14:44:31	Source	[Sent Items]
		From → To	iaman.informant@nist.gov → spy.conspirator@nist.gov
		Subject	RE: Hello, Iaman
		Body	Successfully secured. --------------------------- **From**: spy **Sent**: Monday, March 23, 2015 1:29 PM **To**: iaman **Subject**: Hello, Iaman How are you doing?
	2015-03-23 15:14:58	Source	[Inbox]
		From → To	spy.conspirator@nist.gov → iaman.informant@nist.gov
		Subject	Good job, buddy.
		Body	Good, job. I need a more detailed data about this business.
	2015-03-23 15:20:41	Source	[Inbox]
		From → To	spy.conspirator@nist.gov → iaman.informant@nist.gov
		Subject	RE: Good job, buddy.
		Body	Okay, I got it. I'll be in touch.

		-------------------------- **From**: iaman **Sent**: Monday, March 23, 2015 3:19 PM **To**: spy **Subject**: RE: Good job, buddy. This is a sample. -------------------------- **From**: spy **Sent**: Monday, March 23, 2015 3:15 PM **To**: iaman **Subject**: Good job, buddy. Good, job. I need a more detailed data about this business.	
2015-03-23 15:26:22	Source	[Inbox]	
	From → To	spy.conspirator@nist.gov → iaman.informant@nist.gov	
	Subject	Important request	
	Body	I confirmed it. But, I need a more data. Do your best.	
2015-03-23 15:27:05	Source	[Sent Items]	
	From → To	iaman.informant@nist.gov → spy.conspirator@nist.gov	
	Subject	RE: Important request	
	Body	Umm….. I need time to think. -------------------------- **From**: spy **Sent**: Monday, March 23, 2015 3:26 PM **To**: iaman **Subject**: Important request I confirmed it. But, I need a more data. Do your best.	
2015-03-23 16:38:47	Source	*Recovered Item* from unused area of OST file	
	From → To	iaman.informant@nist.gov → spy.conspirator@nist.gov	
	Subject	It's me	
	Body	Use links below, https://drive.google.com/file/d/0Bz0ye6gXtiZaVl8yVU5mWHlGbWc/view?usp=sharing https://drive.google.com/file/d/0Bz0ye6gXtiZaakx6d3R3c0JmM1U/view?usp=sharing	
2015-03-23 16:41:19	Source	[Deleted Items]	
	From → To	spy.conspirator@nist.gov → iaman.informant@nist.gov	
	Subject	RE: It's me	
	Body	I got it. -------------------------- **From**: iaman **Sent**: Monday, March 23, 2015 4:39 PM **To**: spy **Subject**: It's me Use links below, https://drive.google.com/file/d/0Bz0ye6gXtiZaVl8yVU5mWHlGbWc/view?usp=sharing https://drive.google.com/file/d/0Bz0ye6gXtiZaakx6d3R3c0JmM1U/view?usp=sharing	
2015-03-24 09:25:57	Source	[Inbox]	
	From → To	spy.conspirator@nist.gov → iaman.informant@nist.gov	
	Subject	Last request	
	Body	This is the last request. I want to get the remaining data.	
	Source	[Deleted Items]	
	From → To	iaman.informant@nist.gov → spy.conspirator@nist.gov	

| | 2015-03-24 09:35:10 | Subject | RE: Last request |
| | | Body | This is the last time.. |

The body continues:

From: spy
Sent: Tuesday, March 24, 2015 9:34 AM
To: iaman
Subject: RE: Last request

No problem.
U can directly deliver storage devices that stored it.

From: iaman
Sent: Tuesday, March 24, 2015 9:30 AM
To: spy
Subject: RE: Last request

Stop it!
It is very hard to transfer all data over the internet!

From: spy
Sent: Tuesday, March 24, 2015 9:26 AM
To: iaman
Subject: Last request

This is the last request.
I want to get the remaining data.

	2015-03-24 15:34:02	Source	[Deleted Items]
		From → To	iaman.informant@nist.gov → spy.conspirator@nist.gov
		Subject	RE: Watch out!
		Body	I am trying.

The body continues:

From: spy
Sent: Tuesday, March 24, 2015 3:33 PM
To: iaman
Subject: Watch out!

USB device may be easily detected.

So, try another method.

	2015-03-24 17:05:09	Source	[Deleted Items]
		From → To	iaman.informant@nist.gov → spy.conspirator@nist.gov
		Subject	Done
		Body	It's done. See you tomorrow.
Considerations	- Fortunately, a suspected OST file was not protected and encrypted with a password. - OST file parsing → Inbox, Deleted Items, Contact, and Calendar… - Deleted e-mail recovery from unused area of OST file.		

22) List external storage devices attached to PC.

Possible Answer	Device Name	Volume Name	Serial No.	First Connected Time	Connected Time After Reboot
	SanDisk Cruzer Fit USB Device		4C530012450531101593	2015-03-23 14:31:10 Mon	2015-03-24 09:38:00 Tue
	SanDisk Cruzer Fit USB Device	IAMAN $_@	4C530012550531106501	2015-03-24 09:58:32 Tue	2015-03-24 09:58:33 Tue

Considerations	- 'First Connected Time' can be identified from SetupAPI Log. (→ C:\Windows\inf\setupapi.dev.log)
	
	HKLM\SYSTEM\MountedDevices\
	HKLM\SYSTEM\ControlSet###\Enum\USBSTOR\
	HKLM\SYSTEM\ControlSet###\Control\DeviceClasses\{a5dcbf10-6530-11d2-901f-00c04fb951ed}\
	HKLM\SYSTEM\ControlSet###\Control\DeviceClasses\{53f56307-b6bf-11d0-94f2-00a0c91efb8b}\
	……
	HKU\informant\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\
	HKLM\SOFTWARE\Microsoft\Windows Search\VolumeInfoCache\E:
	   > timestamp: 2015-03-24 09:58:34 Tue
	   > value: VolumeLabel
	   > data: 'IAMAN $_@'
	\Windows\System32\winevt\Logs\System.evtx (Event ID: 20001, 20003…)
	……				

23) Identify all traces related to 'renaming' of files in Windows Desktop.

(It should be considered only during a date range between 2015-03-23 and 2015-03-24.)

[Hint: the parent directories of renamed files were deleted and their MFT entries were also overwritten. Therefore, you may not be able to find their full paths.]

Possible Answer	Timestamp	USN	Path (Of course, just file names are OK)	Event
	2015-03-23 14:41:40	56306184	\Users\informant\Desktop\S data\[secret_project]_detailed_proposal.docx	Renamed Old
		56306328	\Users\informant\Desktop\S data**landscape.png**	Renamed New
(Timezone is applied)	2015-03-23 14:41:55	56307712	\Users\informant\Desktop\S data\[secret_project]_design_concept.ppt	Renamed Old
		56307848	\Users\informant\Desktop\S data**space_and_earth.mp4**	Renamed New
	2015-03-23 16:30:44	58506640	\Users\informant\Desktop\S data\(secret_project)_pricing_decision.xlsx	Renamed Old
		58506776	\Users\informant\Desktop\S data**happy_holiday.jpg**	Renamed New
	2015-03-23 16:31:02	58510288	\Users\informant\Desktop\S data\[secret_project]_final_meeting.pptx	Renamed Old
		58510424	\Users\informant\Desktop\S data**do_u_wanna_build_a_snow_man.mp3**	Renamed New
	2015-03-24 09:49:51	59801680	\Users\informant\Desktop\S data\Secret Project Data\design\ [secret_project]_detailed_design.pptx	Renamed Old
		59801816	\Users\informant\Desktop\S data\Secret Project Data\design\ **winter_whether_advisory.zip**	Renamed New
	2015-03-24 09:50:08	59802408	\Users\informant\Desktop\S data\Secret Project Data\design\ [secret_project]_revised_points.ppt	Renamed Old
		59802544	\Users\informant\Desktop\S data\Secret Project Data\design\ **winter_storm.amr**	Renamed New
	2015-03-24 09:50:49	59803456	\Users\informant\Desktop\S data\Secret Project Data\design\ [secret_project]_design_concept.ppt	Renamed Old
		59803592	\Users\informant\Desktop\S data\Secret Project Data\design\ **space_and_earth.mp4**	Renamed New
	2015-03-24 09:52:35	59814352	\Users\informant\Desktop\S data\Secret Project Data\final\ [secret_project]_final_meeting.pptx	Renamed Old
		59814488	\Users\informant\Desktop\S data\Secret Project Data\final\ **do_u_wanna_build_a_snow_man.mp3**	Renamed New
	2015-03-24 09:52:56	59814904	\Users\informant\Desktop\S data\Secret Project Data\pricing decision\ (secret_project)_market_analysis.xlsx	Renamed Old
		59815040	\Users\informant\Desktop\S data\Secret Project Data\pricing decision\ **new_years_day.jpg**	Renamed New
	2015-03-24 09:53:08	59815232	\Users\informant\Desktop\S data\Secret Project Data\pricing decision\ (secret_project)_market_shares.xls	Renamed Old

		59815360	\Users\informant\Desktop\S data\Secret Project Data\pricing decision\ **super_bowl.avi**	Renamed New
	2015-03-24 09:53:38	59815536	\Users\informant\Desktop\S data\Secret Project Data\pricing decision\ (secret_project)_price_analysis_#1.xlsx	Renamed Old
		59815680	\Users\informant\Desktop\S data\Secret Project Data\pricing decision\ **my_favorite_movies.7z**	Renamed New
	2015-03-24 09:53:52	59815968	\Users\informant\Desktop\S data\Secret Project Data\pricing decision\ (secret_project)_price_analysis_#2.xls	Renamed Old
		59816104	\Users\informant\Desktop\S data\Secret Project Data\pricing decision\ **my_favorite_cars.db**	Renamed New
	2015-03-24 09:54:05	59816312	\Users\informant\Desktop\S data\Secret Project Data\pricing decision\ (secret_project)_pricing_decision.xlsx	Renamed Old
		59816448	\Users\informant\Desktop\S data\Secret Project Data\pricing decision\ **happy_holiday.jpg**	Renamed New
	2015-03-24 09:54:23	59816880	\Users\informant\Desktop\S data\Secret Project Data\progress\ [secret_project]_progress_#1.docx	Renamed Old
		59817008	\Users\informant\Desktop\S data\Secret Project Data\progress\ **my_smartphone.png**	Renamed New
	2015-03-24 09:54:43	59817984	\Users\informant\Desktop\S data\Secret Project Data\progress\ [secret_project]_progress_#2.docx	Renamed Old
		59818112	\Users\informant\Desktop\S data\Secret Project Data\progress\ **new_year_calendar.one**	Renamed New
	2015-03-24 09:54:52	59818320	\Users\informant\Desktop\S data\Secret Project Data\progress\ [secret_project]_progress_#3.doc	Renamed Old
		59818448	\Users\informant\Desktop\S data\Secret Project Data\progress\ **my_friends.svg**	Renamed New
	2015-03-24 09:55:08	59818624	\Users\informant\Desktop\S data\Secret Project Data\proposal\ [secret_project]_detailed_proposal.docx	Renamed Old
		59818768	\Users\informant\Desktop\S data\Secret Project Data\proposal\ **a_gift_from_you.gif**	Renamed New
	2015-03-24 09:55:17	59818976	\Users\informant\Desktop\S data\Secret Project Data\proposal\ [secret_project]_proposal.docx	Renamed Old
		59819096	\Users\informant\Desktop\S data\Secret Project Data\proposal\ **landscape.png**	Renamed New
	2015-03-24 09:55:32	59819272	\Users\informant\Desktop\S data\Secret Project Data\technical review\ [secret_project]_technical_review_#1.docx	Renamed Old
		59819416	\Users\informant\Desktop\S data\Secret Project Data\technical review\ **diary_#1d.txt**	Renamed New
	2015-03-24 09:55:42	59819592	\Users\informant\Desktop\S data\Secret Project Data\technical review\ [secret_project]_technical_review_#1.pptx	Renamed Old
		59819736	\Users\informant\Desktop\S data\Secret Project Data\technical review\ **diary_#1p.txt**	Renamed New
	2015-03-24 09:55:53	59819912	\Users\informant\Desktop\S data\Secret Project Data\technical review\ [secret_project]_technical_review_#2.docx	Renamed Old
		59820056	\Users\informant\Desktop\S data\Secret Project Data\technical review\ **diary_#2d.txt**	Renamed New
	2015-03-24 09:56:09	59823280	\Users\informant\Desktop\S data\Secret Project Data\technical review\ [secret_project]_technical_review_#2.ppt	Renamed Old
		59823424	\Users\informant\Desktop\S data\Secret Project Data\technical review\ **diary_#2p.txt**	Renamed New
	2015-03-24 09:56:14	59823600	\Users\informant\Desktop\S data\Secret Project Data\technical review\ [secret_project]_technical_review_#3.doc	Renamed Old
		59823744	\Users\informant\Desktop\S data\Secret Project Data\technical review\ **diary_#3d.txt**	Renamed New
	2015-03-24 09:56:20	59823920	\Users\informant\Desktop\S data\Secret Project Data\technical review\ [secret_project]_technical_review_#3.ppt	Renamed Old
		59824064	\Users\informant\Desktop\S data\Secret Project Data\technical review\ **diary_#3p.txt**	Renamed New
Considerations	- NTFS journal file analysis (→ $UsnJrnl) - \$Extend\$UsnJrnl·$J (+ $MFT for identifying full paths of files) - With NTFS journal file only, it may be hard to find full paths. - You can consider the Registry ShellBags for further information. - You can also consider the Windows Search database. (See Questions 46)			

24) What is the IP address of company's shared network drive?

Possible Answer	10.11.11.128

Considerations	HKU\informant\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU\
	    > timestamp: 2015-03-23 16:23:28 Mon
	    > value: b
	    > data: '\\10.11.11.128\secured_drive'
	
	HKU\informant\Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU\
	    > timestamp: 2015-03-23 16:26:04 Mon
	    > value: a
	    > data: '\\10.11.11.128\secured_drive'
	
	HKU\informant\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\8\0\
	……

25) List all directories that were traversed in 'RM#2'.

Possible Answer	Timestamp	Directory Path	Source
(Timezone is applied)	2015-03-24 10:00:19	E:\Secret Project Data\	ShellBag (created)
	2015-03-24 10:01:11	E:\Secret Project Data\technical review\	ShellBag (created)
	2015-03-24 10:01:14	E:\Secret Project Data\proposal\	ShellBag (created)
	2015-03-24 10:01:15	E:\Secret Project Data\progress\	ShellBag (created)
	2015-03-24 10:01:17	E:\Secret Project Data\pricing decision\	ShellBag (created)
	2015-03-24 10:01:29	E:\Secret Project Data\design\	ShellBag (last accessed)
	2015-03-24 16:54:07	E:\Secret Project Data\	ShellBag (last accessed)
	2015-03-24 16:54:07	E:\Secret Project Data\progress\	ShellBag (last accessed)
Considerations	- 'Timestamp' may not be accurate. - E:\ can be inferred from external storage devices attached to PC in Question 22. - You can consider a created timestamp and a last accessed timestamp of each ShellBag entry. HKU\informant\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\1~ ……		

26) List all files that were opened in 'RM#2'.

Possible Answer	Timestamp	Directory Path	Source
(Timezone is applied)	2015-03-24 10:01:23	E:\Secret Project Data\design\winter_whether_advisory.zip\	JumpList
	2015-03-24 10:01:29	E:\Secret Project Data\design\winter_whether_advisory.zip\ppt\	JumpList
	2015-03-24 10:01:29	E:\Secret Project Data\design\winter_whether_advisory.zip\	ShellBag (created)
Considerations	- Actually, above list shows directories opened in 'RM#2'. - We can infer that a file 'winter_whether_advisory.zip' was opened and traversed in Windows Explorer. - 'Timestamp' may not be accurate. - E:\ can be inferred from external storage devices attached to PC in Question 22. HKU\informant\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\0\1~ \User\informant\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations \User\informant\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations ……		

27) List all directories that were traversed in the company's network drive.

Possible Answer	Timestamp	Directory Path	Source
(Timezone is applied)	2015-03-23 16:24:01	\\10.11.11.128\secured_drive\Common Data\	ShellBag (created)
	2015-03-23 16:24:08	\\10.11.11.128\secured_drive\Past Projects\	ShellBag (created)
	2015-03-23 16:24:12	\\10.11.11.128\secured_drive\Secret Project Data\design\	ShellBag (created)
	2015-03-23 16:24:15	\\10.11.11.128\secured_drive\Secret Project Data\pricing decision\	ShellBag (created)
	2015-03-23 16:24:16	\\10.11.11.128\secured_drive\Secret Project Data\final\	ShellBag (created)
	2015-03-23 16:24:18	\\10.11.11.128\secured_drive\Secret Project Data\technical review\	ShellBag (created)
	2015-03-23 16:24:20	\\10.11.11.128\secured_drive\Secret Project Data\proposal\	ShellBag (created)
	2015-03-23 16:24:27	\\10.11.11.128\secured_drive\Secret Project Data\progress\	ShellBag (created)
	2015-03-23 16:26:53	\\10.11.11.128\secured_drive\Secret Project Data\pricing decision\	JumpList
	2015-03-23 16:26:54	\\10.11.11.128\secured_drive\Secret Project Data\pricing decision\	.LNK (Windows)
	2015-03-23 16:27:24	V:\Secret Project Data\	ShellBag (created)
	2015-03-23 16:27:29	V:\Secret Project Data\final\	ShellBag (created)
	2015-03-23 16:27:33	V:\Secret Project Data\final\	JumpList
	2015-03-23 16:27:33	V:\Secret Project Data\final\	.LNK (Windows)
	2015-03-23 16:28:17	\\10.11.11.128\secured_drive\Secret Project Data\	ShellBag (last accessed)
	2015-03-23 16:28:17	\\10.11.11.128\secured_drive\Secret Project Data\pricing decision\	ShellBag (last accessed)
	2015-03-24 09:47:54	\\10.11.11.128\secured_drive\	ShellBag (last accessed)
	2015-03-24 09:47:54	\\10.11.11.128\secured_drive\Past Projects\	ShellBag (last accessed)
Considerations	- 'Timestamp' may not be accurate. - V:\ is mapped on \\10.11.11.128 HKU\informant\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\8\0\~ \User\informant\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations \User\informant\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations \User\informant\AppData\Roaming\Microsoft\Windows\Recent*.lnk \User\informant\AppData\Roaming\Microsoft\Office\Recent*.lnk ……		

28) List all files that were opened in the company's network drive.

Possible Answer	Timestamp	Directory Path	Source
(Timezone is applied)	2015-03-23 16:26:53	\\10.11.11.128\SECURED_DRIVE\Secret Project Data\ pricing decision\(secret_project)_pricing_decision.xlsx	JumpList
	2015-03-23 16:26:53	\\10.11.11.128\SECURED_DRIVE\Secret Project Data\ pricing decision\(secret_project)_pricing_decision.xlsx	.LNK (Windows)
	2015-03-23 16:26:53	\\10.11.11.128\SECURED_DRIVE\Secret Project Data\ pricing decision\(secret_project)_pricing_decision.xlsx	.LNK (Office)
	2015-03-23 16:26:56	\\10.11.11.128\secured_drive\Secret Project Data\ pricing decision\(secret_project)_pricing_decision.xlsx	Registry (Office)
	2015-03-23 16:27:33	V:\Secret Project Data\final\[secret_project]_final_meeting.pptx	JumpList
	2015-03-23 16:27:33	V:\Secret Project Data\final\[secret_project]_final_meeting.pptx	.LNK (Windows)
	2015-03-23 16:27:37	V:\Secret Project Data\final\[secret_project]_final_meeting.pptx	.LNK (Office)
	2015-03-23 16:27:37	V:\Secret Project Data\final\[secret_project]_final_meeting.pptx	Registry (Office)
Considerations	- V: is mapped on \\10.11.11.128 \User\informant\AppData\Roaming\Microsoft\Windows\Recent*.lnk \User\informant\AppData\Roaming\Microsoft\Office\Recent*.lnk \User\informant\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations \User\informant\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations HKU\informant\Software\Microsoft\Office\15.0\Excel\File MRU HKU\informant\Software\Microsoft\Office\15.0\PowerPoint\File MRU ……		

29) Find traces related to cloud services on PC.

(Service name, log files...)

Possible Answer	Cloud Service	Type	Traces
	Google Drive	File/Dir	\Program Files (x86)\Google\Drive\
	Google Drive	File/Dir	\User\informant\AppData\Google\Drive\user_default\ > sync_config.db (deleted) > snapshot.db (deleted) > sync_log.log …
	Google Drive	File/Dir	\User\informant\Downloads\googledrivesync.exe
	Google Drive	Registry	HKU\informant\Software\Google\Drive
	Google Drive	Registry	HKU\informant\Software\Classes\GoogleDrive.*
	Apple iCloud	File/Dir	\User\informant\Downloads\icloudsetup.exe
Considerations	- Installation directory - Registry (Configuration, Uninstall Information, Autoruns, UserAssist, Classes…)		

30) What files were deleted from Google Drive?

Find the filename and modified timestamp of the file.

[Hint: Find a transaction log file of Google Drive.]

Possible Answer (Timezone is applied)	Timestamp	File name	Modified Time (UTC-05)
	2015-03-23 16:42:17	happy_holiday.jpg	2015-01-30 11:49:20
	2015-03-23 16:42:17	do_u_wanna_build_a_snow_man.mp3	2015-01-29 15:35:14

Considerations	\User\informant\AppData\Google\Drive\user_default\sync_log.log
	> 2015-03-23 16:32:35,072 -0400 INFO pid=2576 4004:LocalWatcher common.aggregator:114 --------> Received event RawEvent(**CREATE**, path=u'\\\\?\\C:\\Users\\informant\\Google Drive**happy_holiday.jpg**', time=1427142755.056, is_dir=False, ino=4503599627374809L, size=440517L, mtime=**1422563714.5256062**, parent_ino=844424930207017L, is_cancelled=<RawEventIsCancelledFlag.FALSE: 0>, backup=<Backup.NO_BACKUP_CONTENT: (False, False)>) None
	> 2015-03-23 16:32:35,086 -0400 INFO pid=2576 4004:LocalWatcher common.aggregator:114 --------> Received event RawEvent(**CREATE**, path=u'\\\\?\\C:\\Users\\informant\\Google Drive**do_u_wanna_build_a_snow_man.mp3**', time=1427142755.072, is_dir=False, ino=1125899906846942L, size=6844294L, mtime=**1422636560.5520115**, parent_ino=844424930207017L, is_cancelled=<RawEventIsCancelledFlag.FALSE: 0>, backup=<Backup.NO_BACKUP_CONTENT: (False, False)>) None
	> 2015-03-23 16:42:17,026 -0400 INFO pid=2576 4004:LocalWatcher common.aggregator:114 --------> Received event RawEvent(**DELETE**, path=u'\\\\?\\C:\\Users\\informant\\Google Drive**happy_holiday.jpg**', time=1427143336.964, ino=4503599627374809L, parent_ino=844424930207017L, affects_gdoc=False, is_cancelled=<RawEventIsCancelledFlag.FALSE: 0>, backup=<Backup.NO_BACKUP_CONTENT: (False, False)>) None
	> 2015-03-23 16:42:17,026 -0400 INFO pid=2576 4004:LocalWatcher common.aggregator:114 --------> Received event RawEvent(**DELETE**, path=u'\\\\?\\C:\\Users\\informant\\Google Drive**do_u_wanna_build_a_snow_man.mp3**', time=1427143336.964, ino=1125899906846942L, parent_ino=844424930207017L, affects_gdoc=False, is_cancelled=<RawEventIsCancelledFlag.FALSE: 0>, backup=<Backup.NO_BACKUP_CONTENT: (False, False)>) None

	\User\informant\AppData\Google\Drive\user_default\snapshot.db
	\User\informant\AppData\Google\Drive\user_default\snapshot.db-wal
	    > These files are deleted because of the logoff activity.
	    > Need to recover records from unused area of SQLite file.
	    > If 'sync_log.log' file is missing, deleted SQLite record recovery should be considered.
	…

31) Identify account information for synchronizing Google Drive.

Possible Answer (Timezone is applied)	Logon Time (from sync_log.log)	Account
	2015-03-23 16:05:32	iaman.informant.personal@gmail.com
Considerations	\User\informant\AppData\Google\Drive\user_default\sync_log.log	

	> 2015-03-23 16:05:32,279 -0400 INFO pid=2576 2828:LaunchThreads common.service.user:64 Initializing User instance with new credentials. **iaman.informant.personal@gmail.com**
	
	\User\informant\AppData\Google\Drive\user_default\sync_config.db
	\User\informant\AppData\Google\Drive\user_default\sync_config.db-wal
	    > These files are deleted because of the logoff activity.
	    > Need to recover records from unused area of SQLite file.
	    > If 'sync_log.log' file is missing, deleted SQLite record recovery should be considered.
	…	

32) What a method (or software) was used for burning CD-R?

Possible Answer	Windows default CD/DVD burning feature (→ No 3rd party application was used for burning CD-R)

Considerations	- http://windows.microsoft.com/en-us/windows-vista/burn-a-cd-or-dvd
	    > Burning Type 1: Like a USB flash drive
	    > Burning Type 2: With a CD/DVD/ player (Mastered)
	
	- System event logs (for burning type 2 only)
	    > Event IDs for Windows Vista or higher
	     : 113 (cdrom)
	
	- Default burning directory (for burning type 2 only)
	    > \User\informant\AppData\Local\Microsoft\Windows\Burn\Burn
	
	- NTFS journal file analysis (for burning type 2 only)
	    > \$LogFile
	    > \$Extend\\$UsnJrnl·\$J (+ \$MFT for identifying full paths of files)
	    > DAT#####.tmp, DAT#####.tmp, FIL#####.tmp, POST#####.tmp
	……

33) When did the suspect burn CD-R?

[Hint: It may be one or more times.]

Possible Answer	Timestamp	Source	Description
(<u>Timezone is applied</u>)	2015-03-24 15:47:47	\$UsnJrnl	Burning Type 2: With a CD/DVD/ player (Mastered) -------------------- > DAT67383.tmp, DAT34216.tmp > FIL39751.tmp, POST39751.tmp
	2015-03-24 15:47:47	Event Log (System)	Burning Type 2: With a CD/DVD/ player (Mastered)
	2015-03-24 15:56:01	\$UsnJrnl	Burning Type 2: With a CD/DVD/ player (Mastered) -------------------- > DAT32224.tmp, DAT08538.tmp > FIL66692.tmp, POST66692.tmp
	2015-03-24 15:56:11	Event Log (System)	Burning Type 2: With a CD/DVD/ player (Mastered)
	2015-03-24 16:24:19	\$UsnJrnl	Burning Type 2: With a CD/DVD/ player (Mastered) -------------------- > DAT67829.tmp, DAT74017.tmp > FIL51898.tmp, POST51898.tmp
	2015-03-24 16:24:46	Event Log (System)	Burning Type 2: With a CD/DVD/ player (Mastered)
	2015-03-24 16:41:21	Event Log (System)	Burning Type 2: With a CD/DVD/ player (Mastered) -------------------- > DAT85234.tmp, DAT11399.tmp > FIL61821.tmp, POST61821.tmp
	2015-03-24 16:41:21	Event Log (System)	Burning Type 2: With a CD/DVD/ player (Mastered)
	2015-03-24 16:53:16	Registry (Burning Option)	Selecting the method 'Type 1: Like a USB flash drive' -------------------- > A registry key was updated because the suspect selected a new method for burning CD-R > It can be inferred from timestamps of RM#3 image
	2015-03-24 16:53:17	RM#3 image	Formatting Type 1: Like a USB flash drive

	2015-03-24 16:54 ~ 16:58	RM#3 image	Burning Type 1: Like a USB flash drive -------------------- > Creating 17 confidential files > Renaming files > Creating 3 meaningless files > Deleting 17 confidential files

Considerations	- http://windows.microsoft.com/en-us/windows-vista/burn-a-cd-or-dvd
	       > Burning Type 1: Like a USB flash drive
	       > Burning Type 2: With a CD/DVD/ player (Mastered)
	         → System event logs, burning directory, journal logs…
	
	- System event logs (for burning type 2 only)
	       > Event IDs for Windows Vista or higher
	        : 113 (cdrom)
	
	- Default burning directory (for burning type 2 only)
	       > \User\informant\AppData\Local\Microsoft\Windows\Burn\Burn
	       > NTFS Journal Logs
	       > Deleted MFT entry
	       > Registry ShellBag
	       > NFTS INDX slack
	
	- NTFS journal file analysis (for burning type 2 only)
	       > \$LogFile
	       > \$Extend\$UsnJrnl·$J (+ $MFT for identifying full paths of files)
	       > DAT#####.tmp, DAT#####.tmp, FIL#####.tmp, POST#####.tmp
	
	- CD Burning Options
	       > HKU\informant\Software\Microsoft\Windows\CurrentVersion\Explorer\CD Burning\
	         > If the last selection is burning type 1, 'DefaultToMastered' value will be 0.
	         > If the last selection is burning type 2, 'DefaultToMastered' value will be 1.
	
	- Traces of mounting a CD volume for both burning types
	       > Windows .LNK
	       > Jumplist
	       > …
	
	- How to find more traces of burning type 1 on PC?
	       > Is there a solution? It's up to you!
	
	- UDF (Universal Disk Format, http://www.osta.org/specs/pdf/udf260.pdf)
	       > Timestamps stored in descriptors of UDF (ECMA 167 1/7.3)
	       > ex) file offset 0x1017A of RM#3
	
	``
	00010160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
	00010170 00 00 00 00 00 00 00 00 10 1F DF 07 03 18 10 35 ....ß....5
	00010180 11 58 05 00 00 2A 4D 69 63 72 6F 73 6F 66 74 20 .X...*Microsoft
	00010190 57 69 6E 64 6F 77 73 00 00 00 00 06 00 00 00 00 Windows.........
	``
	       > DF 07 (2015), 03 (03), 18 (24), 10 (16), 35 (53), 11 (17)…
	       > 2015-03-24 16:53:17 – Format time of UDF
	……

34) What files were copied from PC to CD-R?

[Hint: Just use PC image only. You can examine transaction logs of the file system for this task.]

Possible Answer	\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\de\
	       > winter_storm.amr
	       > winter_whether_advisory.zip
	
	\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\pd\
	       > my_favorite_cars.db

	> my_favorite_movies.7z > new_years_day.jpg > super_bowl.avi \Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\prog\ 　　> my_friends.svg 　　> my_smartphone.png 　　> new_year_calendar.one \Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\prop\ 　　> a_gift_from_you.gif 　　> landscape.png \Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\tr\ 　　> diary_#1d.txt 　　> diary_#1p.txt 　　> diary_#2d.txt 　　> diary_#2p.txt 　　> diary_#3d.txt 　　> diary_#3p.txt \Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\ 　　> Penguins.jpg 　　> Koala.jpg 　　> Tulips.jpg
Considerations	- It can be inferred from traces of burning type 2 and Question 35. - Traces related to a burning directory (for burning type 2 only) 　　> \User\informant\AppData\Local\Microsoft\Windows\Burn\Burn - NTFS journal file analysis (for burning type 2 only) 　　> \$Extend\$UsnJrnl·$J　(+ $MFT for identifying full paths of files)

35) What files were opened from CD-R?

Possible Answer	Timestamp	File (or Directory) Path	Source
(Timezone is applied)	2015-03-24 16:44:13	D:\de\winter_whether_advisory.zip\	JumpList
	2015-03-24 16:44:14	D:\de\winter_whether_advisory.zip\ppt\	JumpList
	2015-03-24 16:44:16	D:\de\winter_whether_advisory.zip\ppt\slides\	JumpList
	2015-03-24 16:44:18	D:\de\winter_whether_advisory.zip\ppt\slideMasters\	JumpList
	2015-03-24 16:44:18	D:\de\winter_whether_advisory.zip	.LNK (Windows)
	2015-03-24 17:01:10	D:\Penguins.jpg	.LNK (Windows)
	2015-03-24 17:01:12	D:\Koala.jpg	.LNK (Windows)
	2015-03-24 17:01:14	D:\Tulips.jpg	.LNK (Windows)
Considerations	\User\informant\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations \User\informant\AppData\Roaming\Microsoft\Windows\Recent*.lnk ……		

36) Identify all timestamps related to a resignation file in Windows Desktop.

[Hint: the resignation file is a DOCX file in NTFS file system.]

Possible Answer	Timestamp	Type	Source
(Timezone is applied)	2015-03-24 14:48:40	File Created	NTFS MFT Entry $STANDARD_INFORMATION attribute
	2015-03-24 14:59:30	File Modified	
	2015-03-24 14:59:30	Last Accessed	
	2015-03-24 14:59:30	Entry Modified	
	2015-03-24 14:48:40	File Created	NTFS MFT Entry $FILE_NAME attribute
	2015-03-24 14:59:30	File Modified	
	2015-03-24 14:59:30	Last Accessed	
	2015-03-24 14:59:30	Entry Modified	
	2015-03-24 14:32:00	File Created	OOXML \docProps\core.xml
	2015-03-24 14:59:00	File Modified	
Considerations	- External timestamps (→ NTFS File system) - Internal timestamps (→ OOXML)		

37) How and when did the suspect print a resignation file?

Possible Answer	Type	Description
(Timezone is applied)	How	Printed to XPS format
	When	2015-03-25 11:28:34
	Where	\Users\informant\Desktop\Resignation_Letter_(Iaman_Informant).xps

Considerations	- There are no real printer devices.
	 - A XPS file can be found in Windows Desktop.
	
	 HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Printers\
	     > Fax
	       > Microsoft XPS Document Writer
	 …	

38) Where are 'Thumbcache' files located?

Possible Answer	\Users\informant\AppData\Local\Microsoft\Windows\Explorer\thumbcache_32.db \Users\informant\AppData\Local\Microsoft\Windows\Explorer\thumbcache_64.db \Users\informant\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db \Users\informant\AppData\Local\Microsoft\Windows\Explorer\thumbcache_idx.db
Considerations	thumbcache_32.db : BMP files for less than or equal to 32x32 thumbcache_64.db : BMP files for less than or equal to 64x64 thumbcache_256.db : JPG or PNG files for less than or equal to 256x256

39) Identify traces related to confidential files stored in Thumbcache. (Include '256' only)

Possible Answer	[Secret Project] final_meeting.pptx *This file is one of Govdocs (http://digitalcorpora.org/corpora/govdocs) The first page is added by NIST CFReDS project. All following pages have no connection with to the scenario.*	[Secret Project] revised_points.ppt *This file is one of Govdocs (http://digitalcorpora.org/corpora/govdocs) The first page is added by NIST-CFReDS project. All following pages have no connection with to the scenario.*	[Secret Project] detailed_design.pptx *This file is one of Govdocs (http://digitalcorpora.org/corpora/govdocs) The first page is added by NIST-CFReDS project. All following pages have no connection with to the scenario.*
	[Secret Project] technical_review_#1.pptx *This file is one of Govdocs (http://digitalcorpora.org/corpora/govdocs) The first page is added by NIST CFReDS project. All following pages have no connection with to the scenario.*	[Secret Project] technical_review_#2.ppt *This file is one of Govdocs (http://digitalcorpora.org/corpora/govdocs) The first page is added by NIST-CFReDS project. All following pages have no connection with to the scenario.*	[Secret Project] technical_review_#3.ppt *This file is one of Govdocs (http://digitalcorpora.org/corpora/govdocs) The first page is added by NIST-CFReDS project. All following pages have no connection with to the scenario.*
Considerations	- thumbcache_256.db - Thumbnail images of the first pages in MS PowerPoint files.		

40) Where are Sticky Note files located?

Possible Answer	\Users\informant\AppData\Roaming\Microsoft\Sticky Notes\StickyNotes.snt
Considerations	- Microsoft Compound File Binary File Format > https://msdn.microsoft.com/en-us/library/dd942138.aspx

41) Identify notes stored in the Sticky Note file.

Possible Answer	Timestamp (File Modified)	Content
	2015-03-24 14:31:59	Tomorrow… Everything will be OK…
Considerations	* Timestamp may not be accurate.	

42) Was the 'Windows Search and Indexing' function enabled? How can you identify it?

If it was enabled, what is a file path of the 'Windows Search' index database?

Possible Answer	Search & Indexing	Enabled
	DB File path	C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb
Considerations	HKLM\SOFTWARE\Microsoft\Windows Search\ HKLM\SOFTWARE\Microsoft\Windows Search\Databases\Windows (value: FileName) HKU\informant\Software\Microsoft\Windows Search\ HKLM\SYSTEM\ControlSet001\services\WSearch\ (SearchIndexer service → Start up automatically) …...	

43) What kinds of data were stored in Windows Search database?

Possible Answer	- Internet Explorer History - Microsoft Outlook - Files in %UserProfile% (Excluding 'AppData' directory) - Start Menu (/ProgramData/Microsoft/Windows/Start Menu/) - Sticky Note

Considerations	- Microsoft ESE (Extensible Storage Engine) database format
	- Windows.edb
	    > '*System_ItemFolderPathDisplay*' column
	    > '*System_ItemPathDisplay*' column
	    > '*System_Search_Store*' column (→ file, iehistory, mapi15, StickyNotes…)
	    > '*System_ItemNameDisplay*' column
	    > '*System_ItemName*' column
	    > …

44) Find traces of Internet Explorer usage stored in Windows Search database.

(It should be considered only during a date range between 2015-03-22 and 2015-03-23.)

Possible Answer (Timezone is applied)	Date Modified	Microsoft IE TargetUrl
	2015-03-22 11:09:22	http://windows.microsoft.com/en-us/internet-explorer/ie-8-welcome
	2015-03-22 11:09:23	http://www.msn.com/?ocid=iehp
	2015-03-22 11:09:40	https://www.google.com/?gws_rd=ssl
	2015-03-22 11:09:50	https://www.google.com/search?hl=en&source=hp&q=internet+explorer+11&gbv=2&oq=internet+explorer+11&gs_l=heirloom-hp.3..0l10.5163.7893.0.9562.20.13.0.7.7.0.156.1110.11j2.13.0.msedr...0...1ac.1.34.heirloom-hp..0.20.1250.5j7Xm44tv5w
	2015-03-22 11:09:52	http://www.google.com/url?url=http://windows.microsoft.com/en-us/internet-explorer/download-ie&rct=j&frm=1&q=&esrc=s&sa=U&ei=6ykQVZWLGbeJsQT7goDACg&ved=0CB8QFjAA&usg=AFQjCNEwsIz17kY-jTXbaWPcQDfBbVEi7A
	2015-03-22 11:09:54	http://windows.microsoft.com/en-us/internet-explorer/download-ie
	2015-03-22 11:09:56	http://www.google.com/url?url=http://windows.microsoft.com/en-us/internet-explorer/ie-11-worldwide-languages&rct=j&frm=1&q=&esrc=s&sa=U&ei=6ykQVZWLGbeJsQT7goDACg&ved=0CCoQFjAB&usg=AFQjCNE7UKIWEBiWO2N96IFeo6ZywhRLfw
	2015-03-22 11:10:24	http://windows.microsoft.com/en-us/internet-explorer/ie-11-worldwide-languages
	2015-03-22 11:10:54	https://www.google.com/webhp?hl=en
	2015-03-22 11:10:58	https://www.google.com/chrome/index.html?hl=en&brand=CHNG&utm_source=en-hpp&utm_medium=hpp&utm_campaign=en
	2015-03-22 11:11:06	http://download.microsoft.com/download/7/1/7/7179A150-F2D2-4502-9D70-4B59EA148EAA/IE11-Windows6.1-x64-en-us.exe
	2015-03-22 11:11:16	https://www.google.com/chrome/browser/thankyou.html?brand=CHNG&platform=win&clickonceinstalled=1
	2015-03-23 13:26:33	https://odc.officeapps.live.com/odc/emailhrd?lcid=1033&syslcid=1033&uilcid=1033&app=5&ver=15&build=15.0.4420&p=0&a=1&hm=1&sp=0
	2015-03-23 13:27:49	http://www.microsoft.com/en-us/ie-firstrun/win-7/ie-11/vie
	2015-03-23 13:27:49	http://www.bing.com/search

	2015-03-23 13:27:49	http://go.microsoft.com/fwlink/?LinkId=69157
	2015-03-23 13:28:19	http://www.bing.com/
	2015-03-23 14:07:52	http://www.bing.com/news/search?q=Top Stories&FORM=NSBABR
	2015-03-23 14:07:55	http://www.bing.com/search?q=Top+Stories&FORM=HDRSC1
	2015-03-23 14:07:58	http://www.bing.com/news/search?q=file+sharing+and+tethering&FORM=HDRSC6
	2015-03-23 14:08:00	http://www.bing.com/search?q=file+sharing+and+tethering&qs=n&form=QBLH&pq=file+sharing+and+tethering&sc=0-18&sp=-1&sk=&cvid=171b77e4ffd54b2a92c4e97abf995fe1
	2015-03-23 14:08:18	http://sysinfotools.com/blog/tethering-internet-files-sharing/
	2015-03-23 14:11:13	http://resources.infosecinstitute.com/windows-systems-and-artifacts-in-digital-forensics-part-i-registry/
	2015-03-23 14:12:08	https://technet.microsoft.com/en-us/library/cc162846.aspx
	2015-03-23 14:12:45	https://support.microsoft.com/en-us/kb/308427
	2015-03-23 14:12:52	http://en.wikipedia.org/wiki/Event_Viewer
	2015-03-23 14:13:58	https://msdn.microsoft.com/en-us/library/windows/desktop/dd562212(v=vs.85).aspx
	2015-03-23 14:14:25	http://www.forensicswiki.org/wiki/USB_History_Viewing
	2015-03-23 16:43:48	http://www.bing.com/search?q=external%20device%20and%20forensics&qs=n&form=QBRE&pq=external%20device%20and%20forensics&sc=8-9&sp=-1&sk=&cvid=c30c4b1f36114b1c9bc683838c69823a
	2015-03-23 16:43:50	http://www.bing.com/?FORM=Z9FD1
	2015-03-23 16:43:52	http://www.bing.com/news?FORM=Z9LH3
	2015-03-23 16:44:58	http://www.bing.com/news?q=science+technology+news&FORM=NWBTCB
	2015-03-23 16:45:22	http://www.wired.com/?p=1756538
	2015-03-23 16:45:30	http://www.bing.com/news?q=Soccer+News&FORM=NSBABR
	2015-03-23 16:53:47	http://www.bing.com/news?q=top+stories&FORM=NWRFSH
	2015-03-23 16:55:09	http://www.bing.com/news?q=us+news&FORM=NSBABR
	2015-03-23 16:55:10	http://www.bing.com/news?q=world+news&FORM=NSBABR
	2015-03-23 16:55:17	http://www.bing.com/news?q=local&FORM=NSBABR
	2015-03-23 16:55:18	http://www.bing.com/news?q=entertainment+news&FORM=NSBABR
	2015-03-23 16:55:29	http://www.bing.com/news?q=science+technology+news&FORM=NSBABR
	2015-03-23 16:55:55	http://www.bing.com/news?q=business+news&FORM=NSBABR
	2015-03-23 16:55:56	http://www.bing.com/news?q=political+news&FORM=NSBABR
	2015-03-23 16:55:57	http://www.bing.com/news?q=sports+news&FORM=NSBABR
	2015-03-23 16:55:59	http://www.bing.com/news?q=health+news&FORM=NSBABR

	2015-03-23 16:56:09	http://www.bing.com/news?q=top+stories&FORM=NSBABR
	2015-03-23 16:56:33	http://www.wired.com/2015/03/stealing-data-computers-using-heat/

Considerations	- Microsoft ESE (Extensible Storage Engine) database format
	- Windows.edb
	    > '*System_DateModified*' column
	    > '*Microsoft_IE_TargetUrl*' column	

45) List the e-mail communication stored in Windows Search database.

(It should be considered only during a date range between 2015-03-23 and 2015-03-24.)

Possible Answer (Timezone is applied)	Timestamp	E-Mail Communication	
	2015-03-23 13:29:29	Source	[Inbox]
		From → To	spy.conspirator@nist.gov → iaman.informant@nist.gov
		Subject	Hello, Iaman
		Body	How are you doing?
	2015-03-23 14:44:32	Source	[Sent Items]
		From → To	iaman.informant@nist.gov → spy.conspirator@nist.gov
		Subject	RE: Hello, Iaman
		Body	Successfully secured. --------------------------- **From**: spy **Sent**: Monday, March 23, 2015 1:29 PM **To**: iaman **Subject**: Hello, Iaman How are you doing?
	2015-03-23 15:14:58	Source	[Inbox]
		From → To	spy.conspirator@nist.gov → iaman.informant@nist.gov
		Subject	Good job, buddy.
		Body	Good, job. I need a more detailed data about this business.
	2015-03-23 15:19:22 **(Windows.edb only)**	Source	[Sent Items]
		From → To	iaman.informant@nist.gov → spy.conspirator@nist.gov
		Subject	Good job, buddy.
		Attachment	space_and_earth.mp4
		Body	This is a sample. --------------------------- **From**: spy **Sent**: Monday, March 23, 2015 3:15 PM **To**: iaman **Subject**: Good job, buddy. Good, job. I need a more detailed data about this business.
	2015-03-23 15:20:41	Source	[Inbox]
		From → To	spy.conspirator@nist.gov → iaman.informant@nist.gov
		Subject	RE: Good job, buddy.
		Body	Okay, I got it. I'll be in touch. --------------------------- **From**: iaman **Sent**: Monday, March 23, 2015 3:19 PM **To**: spy **Subject**: RE: Good job, buddy. This is a sample.

		--------------------------- **From**: spy **Sent**: Monday, March 23, 2015 3:15 PM **To**: iaman **Subject**: Good job, buddy. Good, job. I need a more detailed data about this business.

2015-03-23 15:26:22	Source	[Inbox]
	From → To	spy.conspirator@nist.gov → iaman.informant@nist.gov
	Subject	Important request
	Body	I confirmed it. But, I need a more data. Do your best.

2015-03-23 15:27:05	Source	[Sent Items]
	From → To	iaman.informant@nist.gov → spy.conspirator@nist.gov
	Subject	RE: Important request
	Body	Umm….. I need time to think. --------------------------- **From**: spy **Sent**: Monday, March 23, 2015 3:26 PM **To**: iaman **Subject**: Important request I confirmed it. But, I need a more data. Do your best.

2015-03-23 16:38:48	Source	[Sent Items]
	From → To	iaman.informant@nist.gov → spy.conspirator@nist.gov
	Subject	It's me
	Body	Use links below, https://drive.google.com/file/d/0Bz0ye6gXtiZaVl8yVU5mWHlGbWc/view?usp=sharing https://drive.google.com/file/d/0Bz0ye6gXtiZaakx6d3R3c0JmM1U/view?usp=sharing

2015-03-23 16:41:19	Source	[Inbox]
	From → To	spy.conspirator@nist.gov → iaman.informant@nist.gov
	Subject	RE: It's me
	Body	I got it. --------------------------- **From**: iaman **Sent**: Monday, March 23, 2015 4:39 PM **To**: spy **Subject**: It's me Use links below, https://drive.google.com/file/d/0Bz0ye6gXtiZaVl8yVU5mWHlGbWc/view?usp=sharing https://drive.google.com/file/d/0Bz0ye6gXtiZaakx6d3R3c0JmM1U/view?usp=sharing

2015-03-24 09:25:57	Source	[Inbox]
	From → To	spy.conspirator@nist.gov → iaman.informant@nist.gov
	Subject	Last request
	Body	This is the last request. I want to get the remaining data.

2015-03-24 09:30:11 **(Windows.edb only)**	Source	[Sent Items]
	From → To	iaman.informant@nist.gov → spy.conspirator@nist.gov
	Subject	RE: Last request
	Body	Stop it! It is very hard to transfer all data over the internet! --------------------------- **From**: spy **Sent**: Tuesday, March 24, 2015 9:26 AM **To**: iaman

| | | **Subject**: Last request | |
| | | This is the last request.
I want to get the remaining data. | |

2015-03-24 09:33:45 **(Windows.edb only)**	Source	[Inbox]
	From → To	spy.conspirator@nist.gov → iaman.informant@nist.gov
	Subject	RE: Last request
	Body	No problem. U can directly deliver storage devices that stored it. --------------------------- **From**: iaman **Sent**: Tuesday, March 24, 2015 9:30 AM **To**: spy **Subject**: RE: Last request Stop it! It is very hard to transfer all data over the internet! --------------------------- **From**: spy **Sent**: Tuesday, March 24, 2015 9:26 AM **To**: iaman **Subject**: Last request This is the last request. I want to get the remaining data.
2015-03-24 09:35:10	Source	[Sent Items]
	From → To	iaman.informant@nist.gov → spy.conspirator@nist.gov
	Subject	RE: Last request
	Body	This is the last time.. --------------------------- **From**: spy **Sent**: Tuesday, March 24, 2015 9:34 AM **To**: iaman **Subject**: RE: Last request No problem. U can directly deliver storage devices that stored it. --------------------------- **From**: iaman **Sent**: Tuesday, March 24, 2015 9:30 AM **To**: spy **Subject**: RE: Last request Stop it! It is very hard to transfer all data over the internet! --------------------------- **From**: spy **Sent**: Tuesday, March 24, 2015 9:26 AM **To**: iaman **Subject**: Last request This is the last request. I want to get the remaining data.
2015-03-24 15:32:42 **(Windows.edb only)**	Source	[Inbox]
	From → To	spy.conspirator@nist.gov → iaman.informant@nist.gov
	Subject	Watch out!
	Body	USB device may be easily detected. So, try another method.
2015-03-24 15:34:02	Source	[Sent Items]
	From → To	iaman.informant@nist.gov → spy.conspirator@nist.gov
	Subject	RE: Watch out!

		Body	I am trying. ---------------------------- **From**: spy **Sent**: Tuesday, March 24, 2015 3:33 PM **To**: iaman **Subject**: Watch out! USB device may be easily detected. So, try another method.
	2015-03-24 17:05:10	Source	[Sent Items]
		From → To	iaman.informant@nist.gov → spy.conspirator@nist.gov
		Subject	Done
		Body	It's done. See you tomorrow.

Considerations	- Microsoft ESE (Extensible Storage Engine) database format
	- Windows.edb
	    > '*System_ItemPathDisplay*' column
	    > '*System_Message_FromName*' column
	    > '*System_Message_ToAddress*' column
	    > '*System_Message_ToName*' column
	    > '*System_Message_DateSent*' column
	    > '*System_Message_DateReceived*' column
	    > '*System_Message_AttachmentNames*' column
	    > '*System_Search_AutoSummary*' column
	    > '*System_Search_AutoSummary*' column
	    …
	- Some e-mail items can be found only in Windows Search database.		

46) List files and directories related to Windows Desktop stored in Windows Search database.

(Windows Desktop directory: \Users\informant\Desktop\)

Possible Answer	Date Created	Full Path
	2015-03-23 16:05:33	C:\\Users\\informant\\Desktop\\Google Drive.lnk
(Timezone is applied)	2015-03-24 09:40:09	C:\\Users\\informant\\Desktop\\S data\\Secret Project Data\\Secret Project Data\\design\\space_and_earth.mp4
	2015-03-24 09:40:09	C:\\Users\\informant\\Desktop\\S data\\Secret Project Data\\Secret Project Data\\design\\winter_whether_advisory.zip
	2015-03-24 09:40:10	C:\\Users\\informant\\Desktop\\S data\\Secret Project Data\\Secret Project Data\\design\\winter_storm.amr
	2015-03-24 09:40:11	C:\\Users\\informant\\Desktop\\S data\\Secret Project Data\\Secret Project Data\\proposal\\[secret_project]_detailed_proposal.docx
	2015-03-24 09:40:13	C:\\Users\\informant\\Desktop\\S data\\Secret Project Data\\Secret Project Data\\proposal\\[secret_project]_proposal.docx
	2015-03-24 09:47:58	C:\\Users\\informant\\Desktop\\S data\\Secret Project Data\\Secret Project Data\\design\\[secret_project]_detailed_design.pptx
	2015-03-24 09:47:58	C:\\Users\\informant\\Desktop\\S data\\Secret Project Data\\Secret Project Data\\final\\[secret_project]_final_meeting.pptx
	2015-03-24 09:47:58	C:\\Users\\informant\\Desktop\\S data\\Secret Project Data\\Secret Project Data\\pricing decision\\(secret_project)_market_analysis.xlsx
	2015-03-24 09:47:58	C:\\Users\\informant\\Desktop\\S data\\Secret Project Data\\Secret Project Data\\pricing decision\\(secret_project)_market_shares.xls
	2015-03-24 09:47:58	C:\\Users\\informant\\Desktop\\S data\\Secret Project Data\\Secret Project Data\\pricing decision\\(secret_project)_price_analysis_#1.xlsx
	2015-03-24 09:47:59	C:\\Users\\informant\\Desktop\\S data\\Secret Project Data\\Secret Project Data\\proposal
	2015-03-24 14:48:41	C:\\Users\\informant\\Desktop\\Resignation_Letter_(Iaman_Informant).docx

	2015-03-24 15:52:06	C:\\Users\\informant\\Desktop\\temp
	2015-03-24 15:52:36	C:\\Users\\informant\\Desktop\\temp\\IE11-Windows6.1-x64-en-us.exe
	2015-03-24 15:52:47	C:\\Users\\informant\\Desktop\\temp\\Chrysanthemum.jpg
	2015-03-24 15:52:47	C:\\Users\\informant\\Desktop\\temp\\Hydrangeas.jpg
	2015-03-24 15:52:47	C:\\Users\\informant\\Desktop\\temp\\Desert.jpg
	2015-03-24 15:52:47	C:\\Users\\informant\\Desktop\\temp\\Lighthouse.jpg
	2015-03-24 15:52:47	C:\\Users\\informant\\Desktop\\temp\\Koala.jpg
	2015-03-24 15:52:47	C:\\Users\\informant\\Desktop\\temp\\Jellyfish.jpg
	2015-03-24 15:52:47	C:\\Users\\informant\\Desktop\\temp\\Tulips.jpg
	2015-03-24 15:52:47	C:\\Users\\informant\\Desktop\\temp\\Penguins.jpg

Considerations	- Microsoft ESE (Extensible Storage Engine) database format
	 - Windows.edb
	  > '*System_DateCreated*' column
	  > '*System_ItemDate*' column
	  > '*System_ItemPathDisplay*' column
	  > '*System_Search_AutoSummary*' column
	  …	

47) Where are Volume Shadow Copies stored? When were they created?

Possible Answer	There is a Volume Shadow Copy in '\System Volume Information\' directory
	
	 \System Volume Information\{9b365826-d2ef-11e4-b734-000c29ff2429}{*Global GUID*}
	  > Created Time: 2015-03-25 10:57:27 AM (Timezone is applied)
	  > File size: 320 MB (335,544,320 bytes)

Considerations	- \System Volume Information\{*Random GUID for a VSC*}{*VSS identifier - Common GUID for VSCs*}
	
	 - VSS identifier stored at file offset 0 for 16 bytes
	  > {3808876b-c176-4e48-b7ae-04046e6cc752}
	  > Global GUID for VSS
	
	 - Shadow Copy ID stored at file offset 144 for 16 bytes
	  > {8f1a2a2d-ce6b-42a5-b92b-f13e65d9c2cb}
	
	 - Shadow Copy set ID stored at file offset 160 for 16 bytes
	  > {56e43eb5-ac18-4f06-a521-1e17712b7ced}
	 …

48) Find traces related to Google Drive service in Volume Shadow Copy. What are the differences between the current system image (of Question 29 ~ 31) and its VSC?

Possible Answer (Timezone is applied)	Date Created	Date Modified	Path	Size	Format
	2015-03-23 16:02:51	2015-03-23 16:47:55	\User\informant\AppData\Google\Drive \user_default**snapshot.db**	20 KB	SQLite
	2015-03-23 16:02:51	2015-03-23 16:47:55	\User\informant\AppData\Google\Drive \user_default**sync_config.db**	11 KB	SQLite
	2015-03-23 16:02:51	2015-03-23 16:47:56	\User\informant\AppData\Google\Drive \user_default**sync_log.log**	341 KB	TEXT

	[Current system image *vs.* VSC] - The last log inside *sync_log.log* from VSC was added at 2015-03-23 16:47:56. - Two SQLite files (*snapshot.db* and *sync_config.db*) exist in VSC. - These files were deleted because of the logoff activity in 2015-03-25. - In other words, VSC was created before the logoff activity.
Considerations	- Creation time of a Volume Shadow Copy > 2015-03-25 10:57:27 AM

49) What files were deleted from Google Drive?

Find deleted records of *cloud_entry* table inside *snapshot.db* from VSC.

(Just examine the SQLite database only. Let us suppose that a text based log file was wiped.)

[Hint: DDL of *cloud_entry* table is as follows.]

CREATE TABLE *cloud_entry*

(doc_id **TEXT**, filename **TEXT**, modified **INTEGER**, created **INTEGER**, acl_role **INTEGER**, doc_type **INTEGER**, removed **INTEGER**, size **INTEGER**, checksum **TEXT**, shared **INTEGER**, resource_type **TEXT**, PRIMARY KEY (doc_id));

Possible Answer	Record Info	Column	Size (bytes)	Data
		doc_id	(69-13)/2 = 28	0Bz0ye6gXtiZaVl8yVU5mWHlGbWc
	[File offset 0x702]	Filename	(75-13)/2 = 31	do_u_wanna_build_a_snow_man.mp3
		modified	4	0x54CBB610 (1422636560) → 2015-01-30 11:49:20 (UTC-05)
	RecordSize: 0x76 RowID: 0x03 HeaderSize: 0x0C	created	4	0x5510786D (1427142765) → 2015-03-23 16:32:45 (UTC-04)
		acl_role	0	0
		doc_type	0	1
		removed	0	0
		size	3	0x686F86 (6844294) → 6,844,294 bytes
		checksum	(77-13)/2 = 32	2c4553f99533d85adb104b3a5c38521a
		shared	0	1
		resource_type	(21-13)/2 = 4	file
		doc_id	fixed size (28)	0Bz0ye6gXtiZaakx6d3R3c0JmM1U
	[File offset 0x77A]	Filename	(47-13)/2 = 17	happy_holiday.jpg
		modified	4	0x54CA9982 (1422563714) → 2015-01-29 15:35:14 (UTC-05)
	First 4 bytes are overwritten	created	4	0x5510786A (1427142762) → 2015-03-23 16:32:42 (UTC-04)
	RecordSize: N/A RowID: N/A HeaderSize: N/A	acl_role	0	0
		doc_type	0	1
		removed	0	0
		size	3	0x6B8C5 (440517) → 440,517 bytes
		checksum	(77-13)/2 = 32	0c77d6a2704155dbfdf29817769b7478
		shared	0	1
		resource_type	(21-13)/2 = 4	file

Considerations	- Deleted SQLite record recovery
	    > http://www.sqlite.org/fileformat2.html
	    > …
	
	- (Deleted record #1) File offset 0x702 of *snapshot.db* from VSC

```
000006F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000700  00 00 76 03 0C 45 4B 04 04 08 03 03 4D 09 15   ..v..EK......M..
00000710  30 42 7A 30 79 65 36 67 58 74 69 5A 61 56 6C 38   0Bz0ye6gXtiZaVl8
00000720  79 56 55 35 6D 57 48 6C 47 62 57 63 64 6F 5F 75   yVU5mWHlGbWcdo_u
00000730  5F 77 61 6E 6E 61 5F 62 75 69 6C 64 5F 61 5F 73   _wanna_build_a_s
00000740  6E 6F 77 5F 6D 61 6E 2E 6D 70 33 54 CB B6 10 55   now_man.mp3TË¶.U
00000750  10 78 6D 68 6F 86 32 63 34 35 35 33 66 39 39 35   .xmho†2c4553f995
00000760  33 33 64 38 35 61 64 62 31 30 34 62 33 61 35 63   33d85adb104b3a5c
00000770  33 38 35 32 31 61 66 69 6C 65 00 00 00 6A 2F 04   38521afile...j/.
00000780  04 08 09 08 03 4D 09 15 30 42 7A 30 79 65 36 67   .....M..0Bz0ye6g
```

- (Deleted record #2) File offset 0x77A of *snapshot.db* from VSC

```
00000760  33 33 64 38 35 61 64 62 31 30 34 62 33 61 35 63   33d85adb104b3a5c
00000770  33 38 35 32 31 61 66 69 6C 65 00 00 00 6A 2F 04   38521afile...j/.
00000780  04 08 09 08 03 4D 09 15 30 42 7A 30 79 65 36 67   .....M..0Bz0ye6g
00000790  58 74 69 5A 61 61 6B 78 36 64 33 52 33 63 30 4A   XtiZaakx6d3R3c0J
000007A0  6D 4D 31 55 68 61 70 70 79 5F 68 6F 6C 69 64 61   mM1Uhappy_holida
000007B0  79 2E 6A 70 67 54 CA 99 82 55 10 78 6A 06 B8 C5   y.jpgTÊ™‚U.xj.,Å
000007C0  30 63 37 37 64 36 61 32 37 30 34 31 35 35 64 62   0c77d6a2704155db
000007D0  66 64 66 32 39 38 31 37 37 36 39 62 37 34 37 38   fdf29817769b7478
000007E0  66 69 6C 65 1A 01 0C 15 15 00 00 00 00 00 00 00   file...........
000007F0  08 19 72 6F 6F 74 72 6F 6F 74 66 6F 6C 64 65 72   ..rootrootfolder
```

50) Why can't we find Outlook's e-mail data in Volume Shadow Copy?

Possible Answer	Outlook OST files were excluded by the following snapshot configuration. HKLM\System\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot\ > OutlookOST: $UserProfile$\AppData\Local\Microsoft\Outlook*.ost
Considerations	- Excluding Files from Shadow Copies > https://msdn.microsoft.com/en-us/library/windows/desktop/aa819132(v=vs.85).aspx

51) Examine 'Recycle Bin' data in PC.

Possible Answer (Timezone is applied)	$I Name	Timestamp Deleted	Original File (or Directory) Path
	$I40295N	2015-03-24 15:51:47	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\prop
	$IXWGVWC	2015-03-24 15:51:47	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\prog
	$I55Z163	2015-03-24 15:51:47	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\pd
	$I9M7UMY	2015-03-24 15:51:47	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\tr
	$I508CBB.jpg	2015-03-24 16:11:42	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Hydrangeas.jpg
	$I8YP3XK.jpg	2015-03-24 16:11:42	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Jellyfish.jpg
	$IDOI3HE.jpg	2015-03-24 16:11:42	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Tulips.jpg
	$IFVCH5V.jpg	2015-03-24 16:11:42	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Penguins.jpg
	$II3FM2A.jpg	2015-03-24 16:11:42	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Desert.jpg
	$IIQGWTT.ini	2015-03-24 16:11:42	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\desktop.ini

	$IJEMT64.exe	2015-03-24 16:11:42	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\IE11-Windows6.1-x64-en-us.exe
	$IKXD1U3.jpg	2015-03-24 16:11:42	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Chrysanthemum.jpg
	$IU3FKWI.jpg	2015-03-24 16:11:42	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Koala.jpg
	$IX538VH.jpg	2015-03-24 16:11:42	C:\Users\informant\AppData\Local\Microsoft\Windows\Burn\Burn\Lighthouse.jpg
Considerations	- The SID of 'informant' account is **1000**. > \$Recycle.Bin\S-1-5-21-2425377081-3129163575-2985601102-**1000*** - Windows 7 Recycle Bin > pairs of **$I**[random].extension & **$R**[random].extension - Although Recycle Bin was emptied in this scenario, the deleted files can be recovered by metadata based data recovery.		

52) What actions were performed for anti-forensics on PC at the last day '2015-03-25'?

	Timestamp	Behavior	Description
Possible Answer (Timezone is applied)	2015-03-25 10:46:44	Search anti-forensic methods	anti-forensic tools
	2015-03-25 10:46:54	Search anti-forensic methods	eraser
	2015-03-25 10:47:34	Download anti-forensic tools	http://iweb.dl.sourceforge.net/project/eraser/Eraser%206/6.2/Eraser%206.2.0.2962.exe
	2015-03-25 10:47:51	Search anti-forensic methods	ccleaner
	2015-03-25 10:48:12	Download anti-forensic tools	http://www.piriform.com/ccleaner/download
	2015-03-25 10:50:14	Install anti-forensic tools	\USERS\INFORMANT\DESKTOP\DOWNLOAD\ERASER 6.2.0.2962.EXE
	2015-03-25 10:57:56	Install anti-forensic tools	\USERS\INFORMANT\DESKTOP\DOWNLOAD\CCSETUP504.EXE
	2015-03-25 11:13:30	Run anti-forensic tools	\PROGRAM FILES\Eraser\Eraser.exe
	2015-03-25 11:13:39 ~ 11:14:44	Wiping files & directories using Eraser	\User\Informant\Desktop\Temp\Chrysanthemum.jpg \User\Informant\Desktop\Temp\Desert.jpg \User\Informant\Desktop\Temp\Hydrangeas.jpg \User\Informant\Desktop\Temp\IE11-Windows6.1-x64-en-us.exe \User\Informant\Desktop\Temp\Jellyfish.jpg \User\Informant\Desktop\Temp\Koala.jpg \User\Informant\Desktop\Temp\Lighthouse.jpg \User\Informant\Desktop\Temp\Penguins.jpg \User\Informant\Desktop\Temp\Tulips.jpg \User\Informant\Desktop\Temp\Tulips.jpg \User\Informant\Desktop\Temp\ (See below)
	2015-03-25 11:15:45	Delete files [Shift] + [Delete]	\Users\informant\Desktop\Download\ccsetup504.exe \Users\informant\Desktop\Download\Eraser 6.2.0.2962.exe
	2015-03-25 11:15:50	Run anti-forensic tools	\PROGRAM FILES\CCLEANER\CCLEANER64.EXE
	2015-03-25 11:18:29	Uninstall anti-forensic tools	\PROGRAM FILES\CCLEANER\UNINST.EXE
	2015-03-25 11:22:47	Disconnecting Google drive account	sync_log.log > 2015-03-25 11:22:47,053 -0400 INFO pid=3164 1528:MainThread common.sync_app:1630 **Signing Out** > 2015-03-25 11:22:48,878 -0400 INFO pid=3164 1528:MainThread common.sync_app:1741 **Deleting file**:

			C:\Users\INFORM~1\AppData\Local\Google\Drive\user_default\sync_config.db > 2015-03-25 11:22:48,878 -0400 INFO pid=3164 1528:MainThread common.sync_app:1741 **Deleting file**: C:\Users\INFORM~1\AppData\Local\Google\Drive\user_default\snapshot.db
	N/A	Delete some e-mails in Outlook	See Question 21 and Question 45. (1) It's me (2) RE: It's me (3) Good job, buddy. (4) RE: Last request (5) Watch out! (6) RE: Watch out! (7) Done

Considerations	[Wiping traces of Eraser in $UsnJrnl]
	- Eraser renames the target file as random bytes, and fills random data.
	    > Current Eraser settings: erasure method (US DoD 5220.22-M → 7 Passes)
	    > (0) Chrysanthemum.jpg (← target file)
	    > (1) S9(wQm9ff_gd/hZ~c (Renamed file for Step 1)
	    > (2) KclInDLFM3YdDX}t1 (Renamed file for Step 2)
	    > (3) C0jAF)No] VBZJoxE (Renamed file for Step 3)
	    > (4) +a]Zd+UuQ88qn/K9J (Renamed file for Step 4)
	    > (5) 2O8josN{78q7Ju7dx (Renamed file for Step 5)
	    > (6) v1hNH f]1bDJc2'(I (Renamed file for Step 6)
	    > (7) 8BkLKk2 cBfQ7`SvH (Renamed file for Step 7)
	    > (8) Delete the last file
	
	- See Question 10 and 11 for identifying application usage logs.
	- See Question 15, 16 and 44 for identifying web history.
	- See Question 30 and 49 for identifying cloud storage drive history.
	……		

53) Recover deleted files from USB drive 'RM#2'.

Possible Answer	Recovery Type	Filename (Path)	Format	Filesize	Viewable
	Metadata (FAT Directory Entry)	\DESIGN\winter_storm.amr	PPT	13.8 MB	O
		\DESIGN\winter_whether_advisory.zip	PPTX	15.6 MB	O
		\pricing decision\my_favorite_cars.db	XLS	1.20 MB	O
		\pricing decision\my_favorite_movies.7z	XLSX	97.7 KB	O
		\pricing decision\new_years_day.jpg	XLSX	9.76 MB	O
		\pricing decision\super_bowl.avi	XLS	9.81 MB	O
		\PROGRESS\my_friends.svg	DOC	57.0 KB	O
		\PROGRESS\my_smartphone.png	DOCX	4.23 MB	O
		\PROGRESS\new_year_calendar.one	DOCX	26.7 KB	O
		\PROPOSAL\a_gift_from_you.gif	DOCX	33.5 MB	O
		\PROPOSAL\landscape.png	DOCX	6.18 MB	O
		\technical review\diary_#1d.txt	DOCX	118 KB	O
		\technical review\diary_#1p.txt	PPTX	447 KB	O
		\technical review\diary_#2d.txt	DOCX	643 KB	O
		\technical review\diary_#2p.txt	PPT	1.10 MB	O
		\technical review\diary_#3d.txt	DOC	2.25 MB	O
		\technical review\diary_#3p.txt	PPT	317 KB	O
	Carving	- All other files do not have a relationship with this scenario. - Results from TestData (PhotoRec) > OGG, 3GP, GIF, JPG, XLS, DOC, MOV, MP4, MPG, PNG, TIF, WMA, WMV, XML…			

Considerations	- Metadata based data recovery 　　　> Directory Entries of FAT file system. 　　　> This task may be enough for 'RM#2' image. - Contents (signatures) based data carving 　　　> This task is optional.

54) What actions were performed for anti-forensics on USB drive 'RM#2'?

[Hint: this can be inferred from the results of Question 53.]

Possible Answer	<u>Quick format</u> for deleting data
Considerations	- Inference from data recovery results. - Some directory entries prior to the quick format do exist in unallocated areas.

55) What files were copied from PC to USB drive 'RM#2'?

Possible Answer (Timezone is applied)	Filename	Format	Filesize	JumpList and ShellBag entry in PC
	winter_storm.amr	PPT	13.8 MB	None
	winter_whether_advisory.zip	PPTX	15.6 MB	E:\Secret Project Data\design\winter_whether_advisory.zip
	my_favorite_cars.db	XLS	1.20 MB	None
	my_favorite_movies.7z	XLSX	97.7 KB	None
	new_years_day.jpg	XLSX	9.76 MB	None
	super_bowl.avi	XLS	9.81 MB	None
	my_friends.svg	DOC	57.0 KB	None
	my_smartphone.png	DOCX	4.23 MB	None
	new_year_calendar.one	DOCX	26.7 KB	None
	a_gift_from_you.gif	DOCX	33.5 MB	None
	landscape.png	DOCX	6.18 MB	None
	diary_#1d.txt	DOCX	118 KB	None
	diary_#1p.txt	PPTX	447 KB	None
	diary_#2d.txt	DOCX	643 KB	None
	diary_#2p.txt	PPT	1.10 MB	None
	diary_#3d.txt	DOC	2.25 MB	None
	diary_#3p.txt	PPT	317 KB	None
Considerations	- Inference from the results of deleted data recovery in Question 53. - Inference from the results of traversed files/directories in Question 25 and 26.			

56) Recover hidden files from the CD-R 'RM#3'.

How to determine proper filenames of the original files prior to renaming tasks?

Possible Answer	Recovery Type	Filename inferred from the First Page & its storage format	Format	Filesize	Viewable
	Data Carving	[secret_project]_revised_points.ppt	PPT	13.8 MB	O
		[secret_project]_detailed_design.pptx	PPTX	15.6 MB	O
		[secret_project]_price_analysis_#1.xlsx	XLSX	97.7 KB	O
		[secret_project]_price_analysis_#2.xls	XLS	1.20 MB	O
		[secret_project]_market_analysis.xlsx	XLSX	9.76 MB	O
		[secret_project]_market_shares.xls	XLS	9.81 MB	O
		[secret_project]_progress_#1.docx	DOCX	4.23 MB	O
		[secret_project]_progress_#2.docx	DOCX	26.7 KB	O
		[secret_project]_progress_#3.doc	DOC	56.0 KB	O
		[secret_project]_detailed_proposal.docx	DOCX	-	Partial
		[secret_project]_proposal.docx	DOCX	6.18 MB	O
		[secret_project]_technical_review_#1.docx	DOCX	118 KB	O

		[secret_project]_technical_review_#1.pptx	PPTX	447 KB	O
		[secret_project]_technical_review_#2.docx	DOCX	643 KB	O
		[secret_project]_technical_review_#2.ppt	PPT	1.10 MB	O
		[secret_project]_technical_review_#3.doc	DOC	2.25 MB	O
		[secret_project]_technical_review_#3.ppt	PPT	317 KB	O

Considerations	- Contents (signatures) based data carving
	    > This task is useful for 'RM#3' image.
	    > Filename can be inferred from the first page and its storage format.
	- Metadata based data recovery
	    > If this task is possible, it may be good for analyst.
	    > With this method, we may be able to identify renamed filenames.
	    > So, additional process is needed for determining original filenames.
	- All other files (some JPEG files) do not have a relationship with this scenario.				

57) What actions were performed for anti-forensics on CD-R 'RM#3'?

Possible Answer	(1) Formatting CD-R (Burning Type 1: Like a USB flash drive) (2) Copying confidential files and some meaningless files to CD-R (3) Deleting confidential files from CD-R for hiding them
Considerations	- This can be inferred from CD-R image examination.

58) Create a detailed timeline of data leakage processes.

Possible Answer	See Section 3

Considerations	- Behavior of the suspect
	    > 2015-03-22: Normal business works (installation and configuration of apps)
	    > 2015-03-23: Transferring sample confidential data through the internet
	    > 2015-03-24: Copying confidential data to storage devices
	    > 2015-03-25: Trying to do anti-forensics and take storage devices out
	- Some traces may be hard to be exactly identified from the images.

59) List and explain methodologies of data leakage performed by the suspect.

Possible Answer	(1) <u>Network Transmission</u>
	    - E-mail
	        > 2015-03-23 15:19 – space_and_earth.mp4
	        > 2015-03-23 16:38 – links of shared files in cloud storage service
	    - Cloud storage services
	        > 2015-03-23 16:32 – happy_holiday.jpg, do_u_wanna_build_a_snow_man.mp3
	
	(2) <u>Storage Device</u>
	    - USB flash drive
	        > 2015-03-24 09:58 ~ 10:00 – winter_whether_advisory.zip and so on
	        > The suspect formatted the partition, but copied files exist in unused area
	    - CD-R
	        > 2015-03-24 16:54 ~ 16:58 – 17 files (e.g., winter_whether_advisory.zip and so on)
	        > The suspect deleted the confidential files, but the files exist in unused area

Considerations	- See Section 5. - See Question 45 related to the e-mail communication. - See Question 30 and 49 related to the cloud storage service. - See Question 22, 25, 26, 54 and 55 related to USB flash drive. - See Question 34 and 56 related to CD-R.

60) Create a visual diagram for a summary of results.

Possible Answer	Graphical Timeline of the Data Leakage Scenario
	- See Section 3 (Graphical Timeline of the Data Leakage Scenario)
Considerations	- A visual diagram of Section 3 is a simple example to better understanding. - You can create your own visual diagram for explaining the results of digital forensic analysis.

7. HISTORY

Rev	Issue Date	Section	History
1.00	2015-06-05	All	- First release version
1.10	2015-09-08	6	- Added additional information about user accounts to Question 6
1.20	2016-11-10	3	- Added additional information about copying files
1.30	2017-12-06	All	- Corrected typing errors - Added additional information about seed files
1.31	2018-03-05	4	- Added a subsection for describing the RM#1 image file
1.32	2018-07-23	6	- For Question 11, updated additional entries from UserAssist, Prefetch and Shimcache, and corrected wrong information (NULL timestamps of several UserAssist entries)