PwC Forensic

Information Technology and Computer Forensics

National Judicial Academy

Strictly Private
and Confidential
Draft

28 August 2016

pwc

Note to the reader

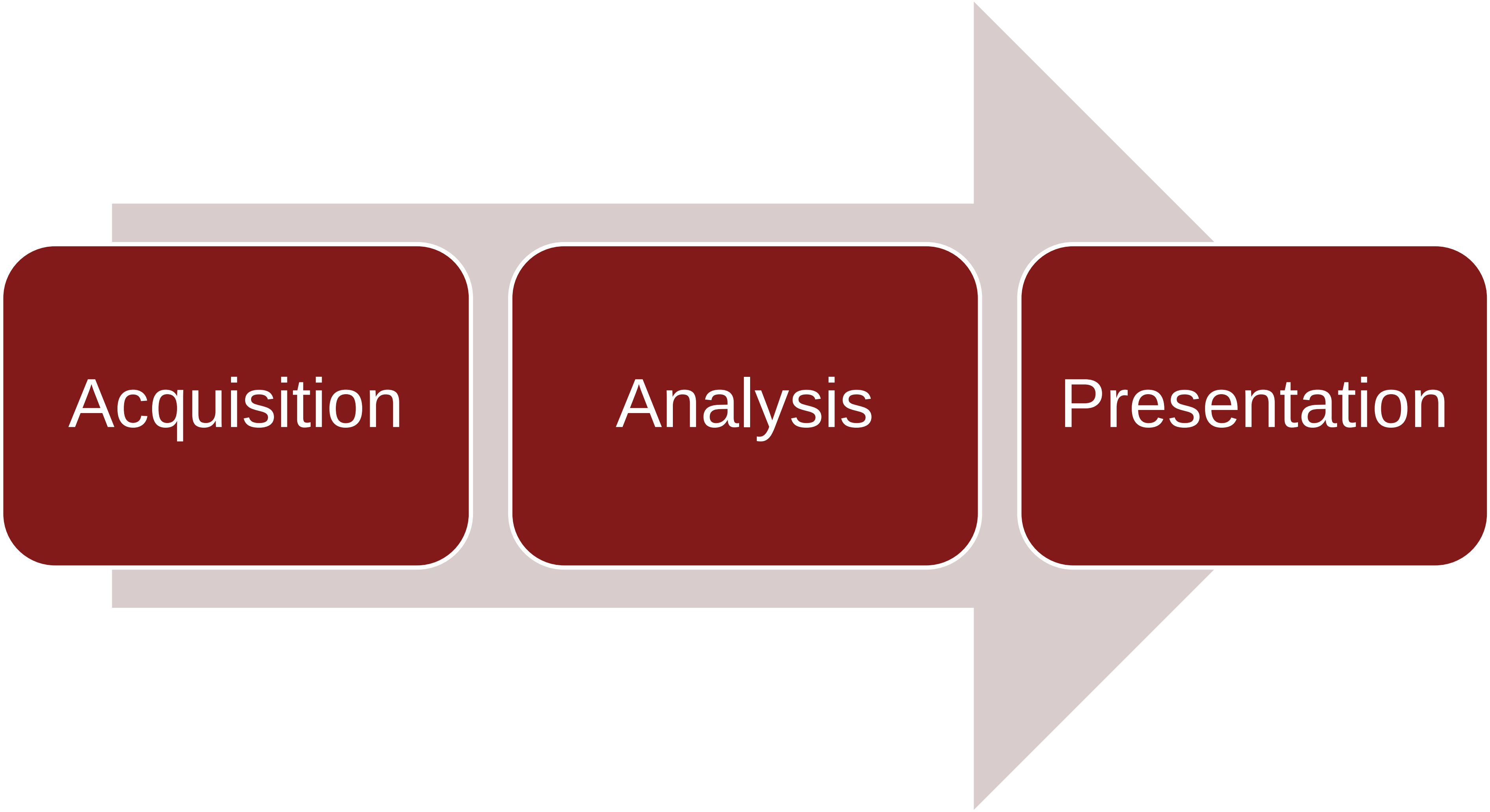
- This presentation has been prepared for “National Judicial Academy” and is not be shared with any external source.
- The views represented in this presentation are purely personal of the presenter and are not to be considered as the view of “Pricewaterhouse Coopers Private Limited”.
- Data from external and public sources have been used to prepare this material.

Agenda

1	Cyber Forensic Life Cycle	3
2	Case Study: 26/11	8
3	Demo: Cyber Forensic Analysis	13

Cyber Forensic Life Cycle

Cyber forensic life cycle



Acquisition

Analysis

Presentation

Acquisition

1. Laptop of ***** *****, a suspect in ******* Blast Case was found in Kanpur on Day 1, seized in Lucknow on Day 2 and sealed in Mumbai on day 4.
2. A threat email was sent using unsecured Wi-Fi connection at ***** in the month ***** of 20** . The wireless router was seized by ***** on the same day. However, no witnesses were present on that day.
3. Two mobile phone were seized from a suspect by ***** Police. They were sealed immediately and sent to FSL. One of the phones contained an external memory card of 4 GB inside. However, it was not mentioned in the forwarding letter to the FSL.
4. For security reasons, all the laptop hard disks of a company are encrypted. One of such computer systems needs to be imaged for investigation.
5. A computer system is strategic to national security. It has been attacked, however can't be shut down and taken to FSL.
6. During an investigation, mail server data of a multinational company needs to be seized. The company maintains its centralized email server in Hong Kong.

Analysis & Presentation

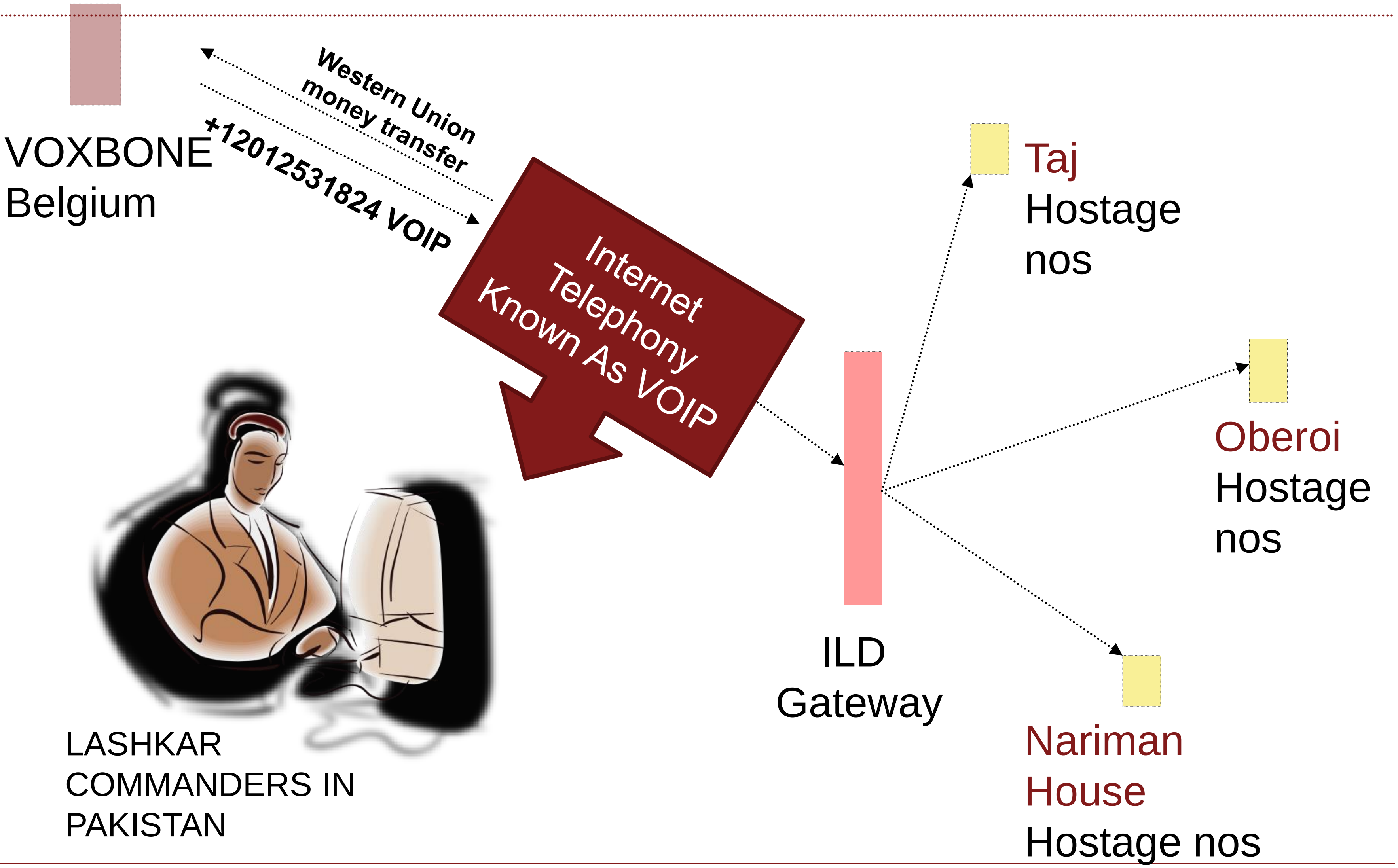
1. A computer hard disk forms an important piece of evidence. However, the integrity of evidence is under question.
2. A video file/ photograph has been submitted as an evidence in the court of law. The defence lawyers alleged that the video file/ photograph was tampered.
3. Few deleted files were retrieved and submitted as an evidence in the court. However, the original file names, path and metadata could not be retrieved.
4. A witness statement indicated that the deceased victim was receiving threats via internet telephony and internet video calls from the potential perpetrators. The mobile of the deceased was password protected, and hence a corroborative evidence was necessary
5. A fake FB profile was created by means of identity theft. The screen shots of the fake profile were submitted as an evidence in the court of law; however the profile was deleted by the time the data was requested from FB. FB conveyed that it did not maintain data of deleted profiles.

Analysis & Presentation

6. An email exhibit was retrieved from sent messages of one of the suspects; however it was not available in the other suspect’s inbox.
7. A CCTV footage was obtained from the scene of crime. The footage was unclear; however the Police arrested suspects who resembled the people seen the CCTV.

Case Study: 26/11

Investigation of 26/11 Mumbai Terror Attack (1 of 4)



VOXBONE Belgium

Western Union money transfer

+12012531824 VOIP

Internet Telephony Known As VOIP

LASHKAR COMMANDERS IN PAKISTAN

ILD Gateway

Taj Hostage nos

Oberoi Hostage nos

Nariman House Hostage nos

Investigation of 26/11 Mumbai Terror Attack (2 of 4)

Testimony of Kasab:

- The 10 terrorists were equipped with a Nokia 1200 phone mobile and a SIM Card by the Pakistani Handlers (i.e. total ten mobiles and ten SIM cards)

Investigation:

- Five of the 10 mobile phones recovered from SoC:
  - **Two in Oberoy** – one with original SIM, one lady victim's SIM
  - **One in Taj**
  - **One in Nariman House** (Gabrian's SIM) and
  - **One unused Mobile:** Recovered during searches at Oberoy
- Imaging and acquisition of mobile phone data
-

Evidence submitted in the court of law:

- FSL Report of Mobile Forensic Analysis (IMEI, MSISDN, Call Logs)
- Testimony of Nokia India Rep from Gurgaon – none of the IMEI sold in India
- Testimony of legal rep of Nokia China (Donga) – two of the five IMEI sold in Pakistan
- Cross examination over Video Conferencing
- Record of interceptions of four IMEI, along with testimony of ATS PI, Mr. N. T. Kadam

Investigation of 26/11 Mumbai Terror Attack (3 of 4)

Testimony of Kasab:

- Terrorists were asked to call on the VIOP no +12012531824 as well as to long-press the green button on Nokia 1200 to speed-dial.

Findings during investigation:

- Gateway interception of calls from four IMEI & Multiple SIMs to the VOIP;
- The VOIP Service Provider, Voxbone Approached;
- The KYC Details were obtained;
- Money Trail was identified towards obtaining of

Evidence submitted in the court of law:

- CDRs of 17 Nos: Confirmed that Internet Calls made during the 26/11 period;
- KYC Records of Voxbone: Subscriber Khadak Singh, India; Passport submitted along with belonged to Pakistan;
- Money Gram Fund Transfers to Voxbone, NJ were traced to Pakistan;
- Testimony of Abu Jundal: He, along with Vasi and Qafa attended calls from Karachi.

Investigation of 26/11 Mumbai Terror Attack (4 of 4)

Challenges:

1. It could **not** be proven basis technical evidence that the handlers of terrorists were receiving VIOP **phones from a Cell Site in Pakistan**, as VOXBONE doesn't maintain any logs without prior notice by LEAs. **(IMPACT: Q-NET issue of Ravi Pujari Gang?)**
2. The Nokia China Legal Rep sent an email to Nokia's India office regarding the connection of Nokia 1200 phones with Pakistan, which was produced before the court. **(Pseudo- 65 B Certificate ?)**
3. CDRs of the intercepted numbers only contained AlphaNumeric codes indicating the internet calls, and not the called VOIP number.
4. **Voice samples of the handlers in Pakistan yet to be made available for forensic analysis.**
5. The KYC documents from VOXBONE as well as the evidence of Money Trail could not be obtained **only because of the effective intervention of FBI**, as the handlers of terrorists had made payment to New Jersey unit of VOXBONE.
6. The Mumbai police officers had to conduct visit to New Jearsey to obtain the KYC documents. **(May happen once in a million cases…)**

Demo: Cyber Forensic Analysis

Digital Forensics Analysis

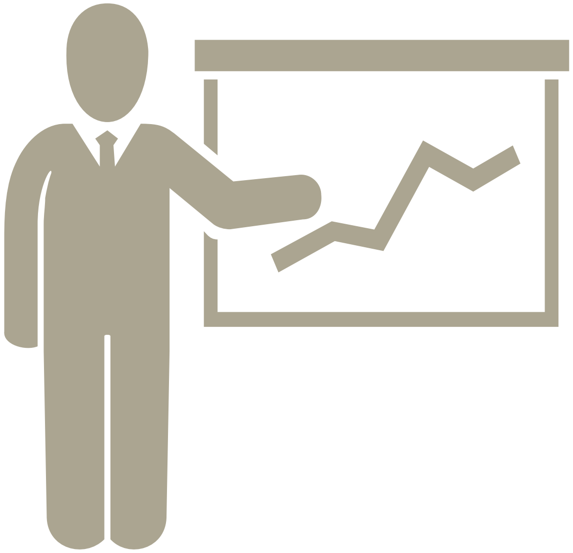
Once the image has been acquired in a forensic manner, computer forensic team starts working on the analysis part. Depending on the scenario, different techniques are applied to look for the evidence on the acquired media.

- Data Carving /Deleted partition / file / folder recovery
- USB activity analysis
- Operating system registry analysis
- Internet history analysis
- Instant messaging log analysis
- Web cache analysis
- File/Folder Metadata analysis. Example EXIF information from picture file.
- Password cracking of files
- Time-line pattern analysis
- Link file analysis and Most Recently used (MRU) files/ folder analysis
- Malicious application installation/ un-installation activity

Practical Demo on using Forensic tools

- Recovering deleted contents and co-relating time stamps
- Recovering a password from protected files
- Recovering web pages/chat information
- Parsing the windows registry files for information's
- Searching for data on the data

And more …



Windows Artefacts provide a chronological sequence of events

Last Accessed

- Displays the last accessed date/time. This typically reflects the last time the operating system or any compliant application touched the file (such as viewing, dragging, or right clicking). Entries on FAT volumes do not have a last accessed time.

File Created

- Typically reflects the date/time the file/folder was created at that location. A notable exception is the extraction of files/folders from a ZIP archive. Those objects carry the created date/time as they existed when the objects were placed in the archive.

Last Written

- Reflects the date/time the file was last opened, edited, then saved.

Entry Modified

- Indicates when the administrative data for the file was last altered for NTFS and Linux.

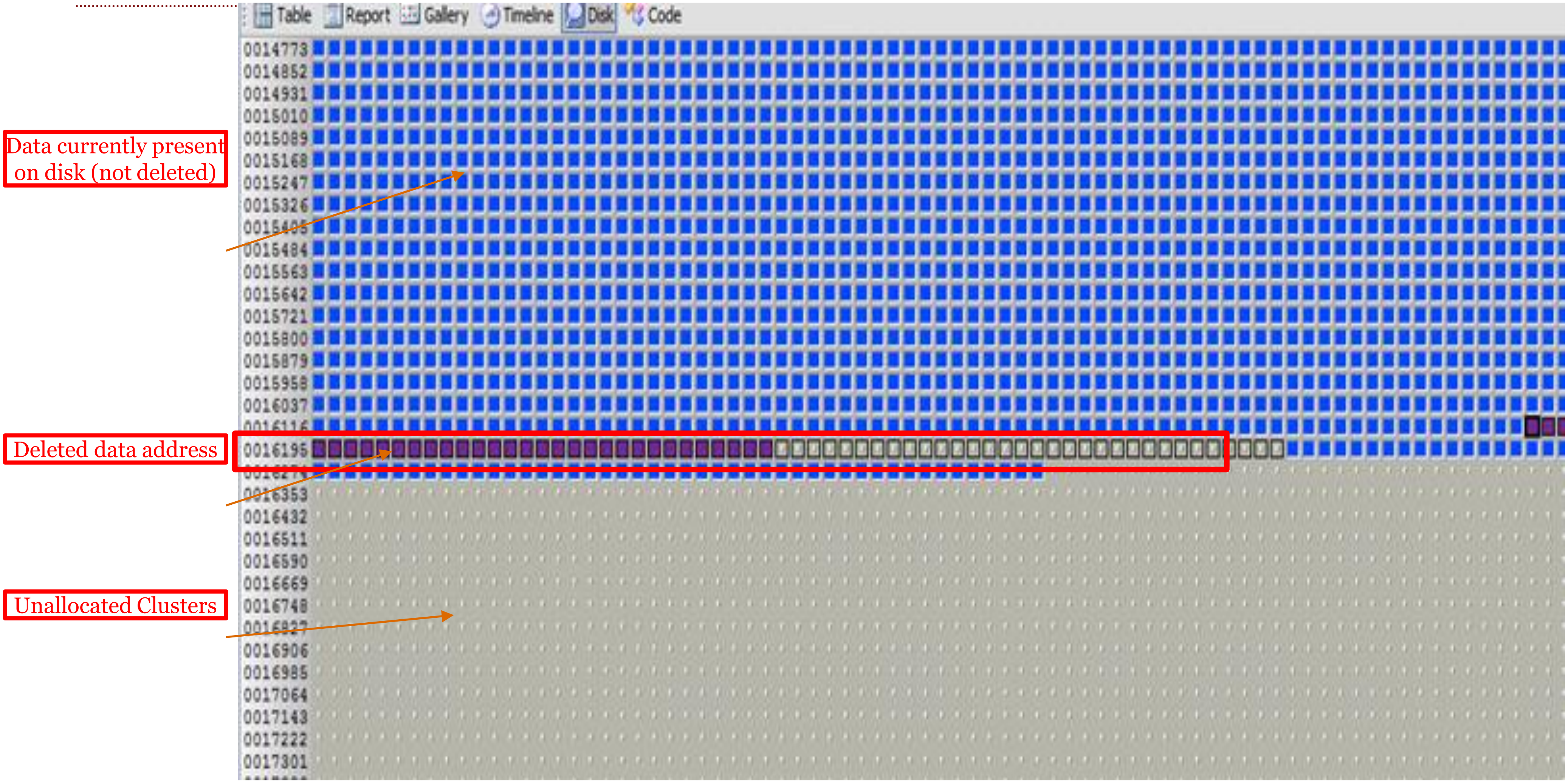
File Deleted

- Shows the deletion time and date of files associated with a Recycle Bin record.

File Acquired

- Displays the date and time the evidence file (where the selected file resides) was acquired.

How a disk looks to a digital forensic investigator



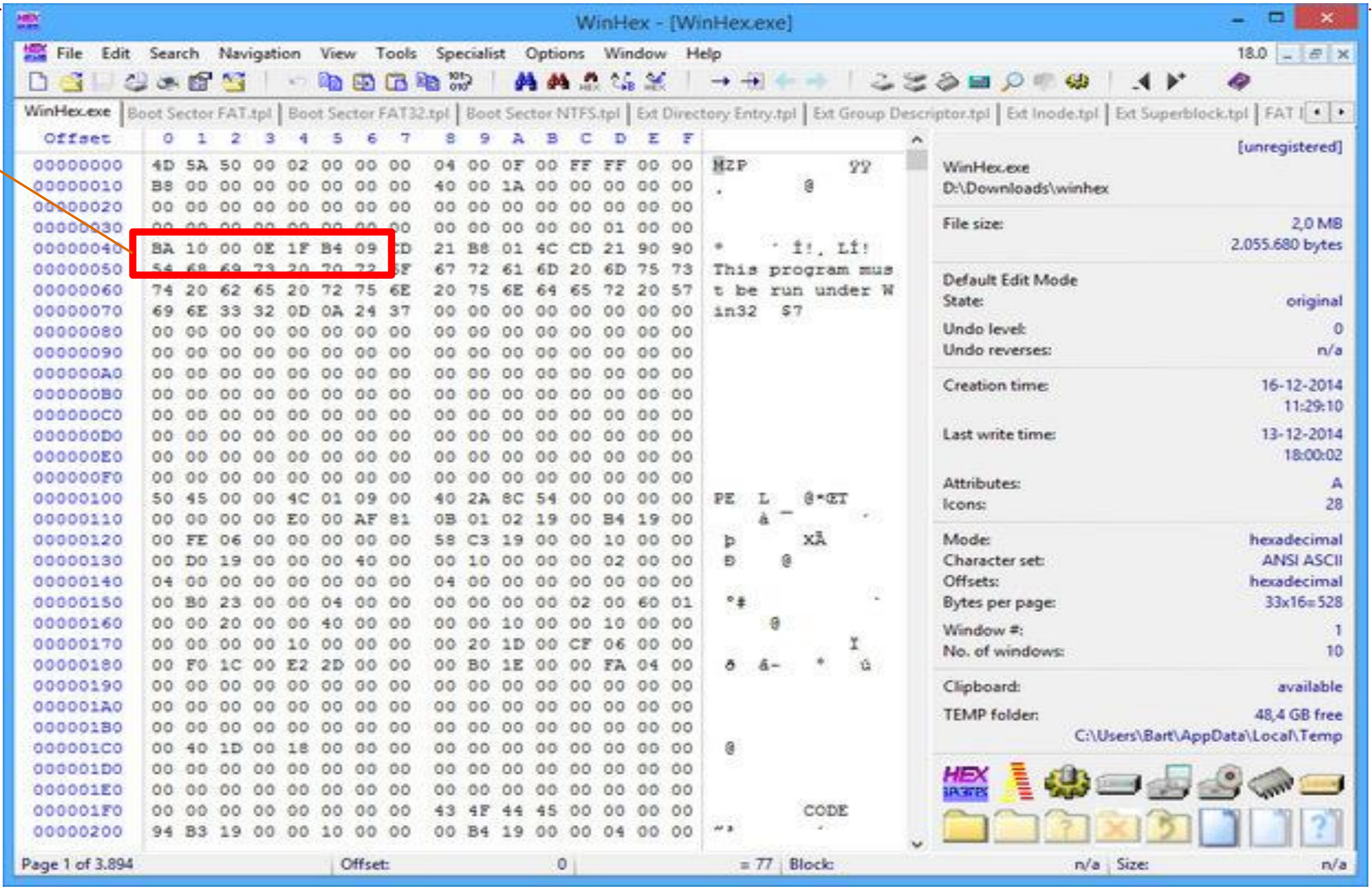
Data currently present on disk (not deleted)

Deleted data address

Unallocated Clusters

Data Recovery using Header and Footer reconstruction

Deleted files are reconstructed using file signatures wherein Headers indicate starting point of the file offset and Footers indicate ending point.



```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F
00000000  4D 5A 50 00 02 00 00 00  04 00 0F 00 FF FF 00 00  MZP         ÿÿ
00000010  B8 00 00 00 00 00 00 00  40 00 1A 00 00 00 00 00  ¸       @
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000030  00 00 00 00 00 00 00 00  00 00 00 00 00 01 00 00
00000040  BA 10 00 0E 1F B4 09 CD  21 B8 01 4C CD 21 90 90  º    ´ Í!¸ LÍ!
00000050  54 68 69 73 20 70 72 6F  67 72 61 6D 20 6D 75 73  This program mus
00000060  74 20 62 65 20 72 75 6E  20 75 6E 64 65 72 20 57  t be run under W
00000070  69 6E 33 32 0D 0A 24 37  00 00 00 00 00 00 00 00  in32  $7
00000080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000C0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000000F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000100  50 45 00 00 4C 01 09 00  40 2A 8C 54 00 00 00 00  PE  L   @*ŒT
00000110  00 00 00 00 E0 00 AF 81  0B 01 02 19 00 B4 19 00      à ¯      ´
00000120  00 FE 06 00 00 00 00 00  58 C3 19 00 00 10 00 00   þ      XÃ
00000130  00 D0 19 00 00 00 40 00  00 10 00 00 00 02 00 00   Ð    @
00000140  04 00 00 00 00 00 00 00  04 00 00 00 00 00 00 00
00000150  00 B0 23 00 00 04 00 00  00 00 00 00 02 00 60 01   °#          `
00000160  00 00 20 00 00 40 00 00  00 00 10 00 00 10 00 00       @
00000170  00 00 00 00 10 00 00 00  00 20 1D 00 CF 06 00 00              Ï
00000180  00 F0 1C 00 E2 2D 00 00  00 B0 1E 00 00 FA 04 00   ð  â-    °   ú
00000190  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001B0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001C0  00 40 1D 00 18 00 00 00  00 00 00 00 00 00 00 00   @
000001D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001F0  00 00 00 00 00 00 00 00  43 4F 44 45 00 00 00 00          CODE
00000200  94 B3 19 00 00 10 00 00  00 B4 19 00 00 04 00 00  ”³       ´
```

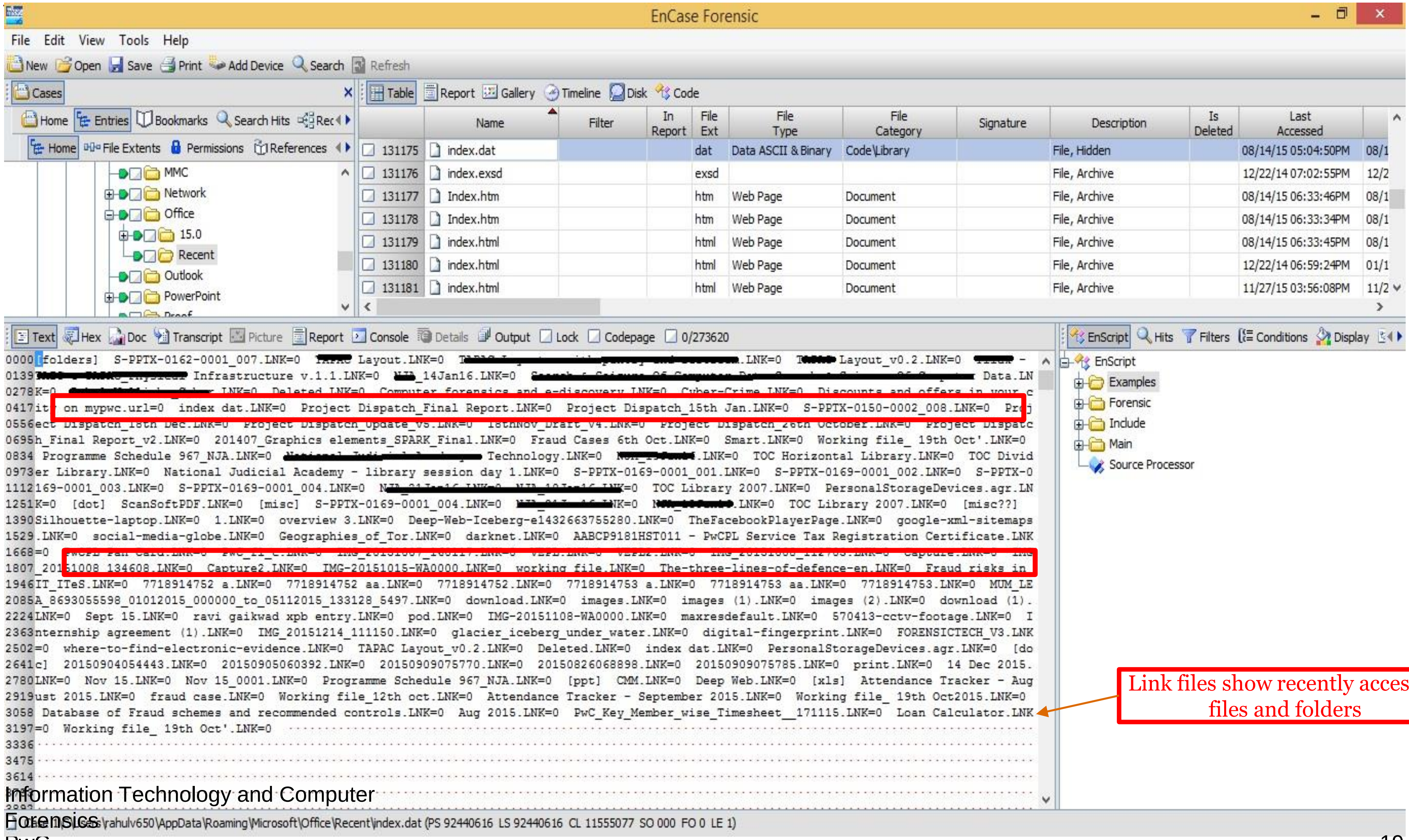
[unregistered]

WinHex.exe
D:\Downloads\winhex

File size:	2,0 MB 2.055.680 bytes
Default Edit Mode	
State:	original
Undo level:	0
Undo reverses:	n/a
Creation time:	16-12-2014 11:29:10
Last write time:	13-12-2014 18:00:02
Attributes:	A
Icons:	28
Mode:	hexadecimal
Character set:	ANSI ASCII
Offsets:	hexadecimal
Bytes per page:	33x16=528
Window #:	1
No. of windows:	10
Clipboard:	available
TEMP folder:	48,4 GB free C:\Users\Bart\AppData\Local\Temp

Page 1 of 3.894 | Offset: 0 | = 77 | Block: n/a | Size: n/a

Pointers to recently accessed files and folders


EnCase Forensic
File Edit View Tools Help
New Open Save Print Add Device Search Refresh
Cases
Home Entries Bookmarks Search Hits Rec
Home File Extents Permissions References
MMC
Network
Office
15.0
Recent
Outlook
PowerPoint
Proof
Table Report Gallery Timeline Disk Code
Text Hex Doc Transcript Picture Report Console Details Output Lock Codepage 0/273620
EnScript Hits Filters Conditions Display
EnScript
Examples
Forensic
Include
Main
Source Processor

	Name	Filter	In Report	File Ext	File Type	File Category	Signature	Description	Is Deleted	Last Accessed	
131175	index.dat			dat	Data ASCII & Binary	Code\Library		File, Hidden		08/14/15 05:04:50PM	08/1
131176	index.exsd			exsd				File, Archive		12/22/14 07:02:55PM	12/2
131177	Index.htm			htm	Web Page	Document		File, Archive		08/14/15 06:33:46PM	08/1
131178	Index.htm			htm	Web Page	Document		File, Archive		08/14/15 06:33:34PM	08/1
131179	index.html			html	Web Page	Document		File, Archive		08/14/15 06:33:45PM	08/1
131180	index.html			html	Web Page	Document		File, Archive		12/22/14 06:59:24PM	01/1
131181	index.html			html	Web Page	Document		File, Archive		11/27/15 03:56:08PM	11/2

```
0000[folders]  S-PPTX-0162-0001_007.LNK=0  [redacted] Layout.LNK=0  [redacted].LNK=0  [redacted] Layout_v0.2.LNK=0  [redacted] -
0139[redacted] Infrastructure v.1.1.LNK=0  [redacted]_14Jan16.LNK=0  [redacted] Data.LN
0278K=0  [redacted].LNK=0  Deleted.LNK=0  Computer forensics and e-discovery.LNK=0  Cyber-Crime.LNK=0  Discounts and offers in your c
0417ity on mypwc.url=0  index dat.LNK=0  Project Dispatch_Final Report.LNK=0  Project Dispatch_15th Jan.LNK=0  S-PPTX-0150-0002_008.LNK=0  Proj
0556ect Dispatch_18th Dec.LNK=0  Project Dispatch_Update_v5.LNK=0  18thNov_Draft_v4.LNK=0  Project Dispatch_26th October.LNK=0  Project Dispatc
0695h_Final Report_v2.LNK=0  201407_Graphics elements_SPARK_Final.LNK=0  Fraud Cases 6th Oct.LNK=0  Smart.LNK=0  Working file_ 19th Oct'.LNK=0
0834 Programme Schedule 967_NJA.LNK=0  [redacted] Technology.LNK=0  [redacted].LNK=0  TOC Horizontal Library.LNK=0  TOC Divid
0973er Library.LNK=0  National Judicial Academy - library session day 1.LNK=0  S-PPTX-0169-0001_001.LNK=0  S-PPTX-0169-0001_002.LNK=0  S-PPTX-0
1112169-0001_003.LNK=0  S-PPTX-0169-0001_004.LNK=0  [redacted]=0  TOC Library 2007.LNK=0  PersonalStorageDevices.agr.LN
1251K=0  [dot]  ScanSoftPDF.LNK=0  [misc]  S-PPTX-0169-0001_004.LNK=0  [redacted]NK=0  [redacted].LNK=0  TOC Library 2007.LNK=0  [misc??]
1390Silhouette-laptop.LNK=0  1.LNK=0  overview 3.LNK=0  Deep-Web-Iceberg-e1432663755280.LNK=0  TheFacebookPlayerPage.LNK=0  google-xml-sitemaps
1529.LNK=0  social-media-globe.LNK=0  Geographies_of_Tor.LNK=0  darknet.LNK=0  AABCP9181HST011 - PwCPL Service Tax Registration Certificate.LNK
1668=0  PwCPL Pan Card.LNK=0  PwC_IT_C.LNK=0  IMG_20151007_160117.LNK=0  VEPL.LNK=0  VEPL2.LNK=0  IMG_20151008_112753.LNK=0  Capture.LNK=0  IMG
1807_20151008 134608.LNK=0  Capture2.LNK=0  IMG-20151015-WA0000.LNK=0  working file.LNK=0  The-three-lines-of-defence-en.LNK=0  Fraud risks in
1946IT_ITeS.LNK=0  7718914752 a.LNK=0  7718914752 aa.LNK=0  7718914752.LNK=0  7718914753 a.LNK=0  7718914753 aa.LNK=0  7718914753.LNK=0  MUM_LE
2085A_8693055598_01012015_000000_to_05112015_133128_5497.LNK=0  download.LNK=0  images.LNK=0  images (1).LNK=0  images (2).LNK=0  download (1).
2224LNK=0  Sept 15.LNK=0  ravi gaikwad xpb entry.LNK=0  pod.LNK=0  IMG-20151108-WA0000.LNK=0  maxresdefault.LNK=0  570413-cctv-footage.LNK=0  I
2363nternship agreement (1).LNK=0  IMG_20151214_111150.LNK=0  glacier_iceberg_under_water.LNK=0  digital-fingerprint.LNK=0  FORENSICTECH_V3.LNK
2502=0  where-to-find-electronic-evidence.LNK=0  TAPAC Layout_v0.2.LNK=0  Deleted.LNK=0  index dat.LNK=0  PersonalStorageDevices.agr.LNK=0  [do
2641c]  20150904054443.LNK=0  20150905060392.LNK=0  20150909075770.LNK=0  20150826068898.LNK=0  20150909075785.LNK=0  print.LNK=0  14 Dec 2015.
2780LNK=0  Nov 15.LNK=0  Nov 15_0001.LNK=0  Programme Schedule 967_NJA.LNK=0  [ppt]  CMM.LNK=0  Deep Web.LNK=0  [xls]  Attendance Tracker - Aug
2919ust 2015.LNK=0  fraud case.LNK=0  Working file_12th oct.LNK=0  Attendance Tracker - September 2015.LNK=0  Working file_ 19th Oct2015.LNK=0
3058 Database of Fraud schemes and recommended controls.LNK=0  Aug 2015.LNK=0  PwC_Key_Member_wise_Timesheet__171115.LNK=0  Loan Calculator.LNK
3197=0  Working file_ 19th Oct'.LNK=0  ..........................................................................
3336.........................................................................................................
3475.........................................................................................................
3614.........................................................................................................
```

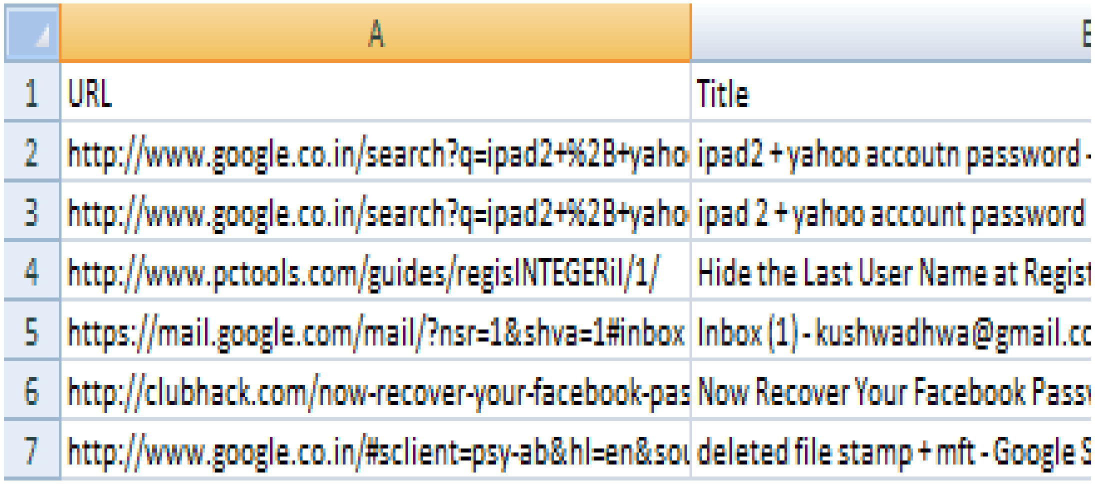
\Users\rahulv650\AppData\Roaming\Microsoft\Office\Recent\index.dat (PS 92440616 LS 92440616 CL 11555077 SO 000 FO 0 LE 1)

Link files show recently accessed files and folders

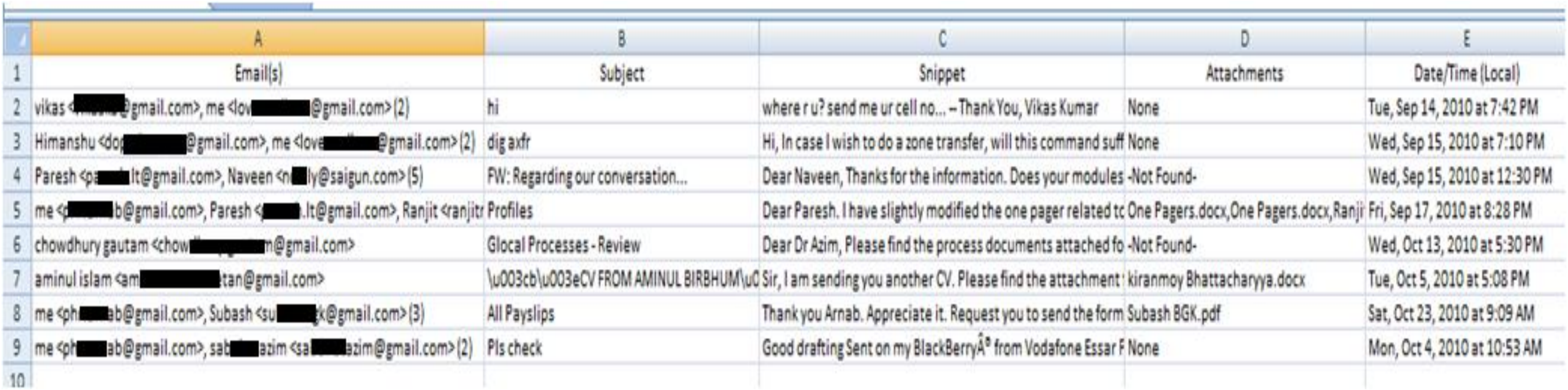
Internet Cache Analysis

Internet Cache Forensics involves gathering evidence from

1. Facebook email / chat/ web page fragments
2. Yahoo email / chat fragments
3. Gmail email / chat fragments
4. Hotmail email fragments
5. Twitter page fragments
6. Pages browsed from Internet explorer, Firefox, Opera, Safari



	A	E
1	URL	Title
2	http://www.google.co.in/search?q=ipad2+%2B+yaho	ipad2 + yahoo accoutn password -
3	http://www.google.co.in/search?q=ipad2+%2B+yaho	ipad 2 + yahoo account password
4	http://www.pctools.com/guides/regisINTEGERil/1/	Hide the Last User Name at Regist
5	https://mail.google.com/mail/?nsr=1&shva=1#inbox	Inbox (1) - kushwadhwa@gmail.cc
6	http://clubhack.com/now-recover-your-facebook-pas	Now Recover Your Facebook Passw
7	http://www.google.co.in/#sclient=psy-ab&hl=en&sou	deleted file stamp + mft - Google S



	A	B	C	D	E
1	Email(s)	Subject	Snippet	Attachments	Date/Time (Local)
2	vikas <[redacted]@gmail.com>, me <lov[redacted]@gmail.com> (2)	hi	where r u? send me ur cell no... -- Thank You, Vikas Kumar	None	Tue, Sep 14, 2010 at 7:42 PM
3	Himanshu <do[redacted]@gmail.com>, me <love[redacted]@gmail.com> (2)	dig axfr	Hi, In case I wish to do a zone transfer, will this command suff	None	Wed, Sep 15, 2010 at 7:10 PM
4	Paresh <pa[redacted]lt@gmail.com>, Naveen <n[redacted]ly@saigun.com> (5)	FW: Regarding our conversation...	Dear Naveen, Thanks for the information. Does your modules	-Not Found-	Wed, Sep 15, 2010 at 12:30 PM
5	me <[redacted]b@gmail.com>, Paresh <[redacted].lt@gmail.com>, Ranjit <ranjitr	Profiles	Dear Paresh. I have slightly modified the one pager related tc	One Pagers.docx,One Pagers.docx,Ranji	Fri, Sep 17, 2010 at 8:28 PM
6	chowdhury gautam <chow[redacted]m@gmail.com>	Glocal Processes - Review	Dear Dr Azim, Please find the process documents attached fo	-Not Found-	Wed, Oct 13, 2010 at 5:30 PM
7	aminul islam <am[redacted]tan@gmail.com>	\u003cb\u003eCV FROM AMINUL BIRBHUM\u0	Sir, I am sending you another CV. Please find the attachment	kiranmoy Bhattacharyya.docx	Tue, Oct 5, 2010 at 5:08 PM
8	me <ph[redacted]ab@gmail.com>, Subash <su[redacted]k@gmail.com> (3)	All Payslips	Thank you Arnab. Appreciate it. Request you to send the form	Subash BGK.pdf	Sat, Oct 23, 2010 at 9:09 AM
9	me <ph[redacted]ab@gmail.com>, sab[redacted]azim <sa[redacted]azim@gmail.com> (2)	Pls check	Good drafting Sent on my BlackBerryÂ® from Vodafone Essar F	None	Mon, Oct 4, 2010 at 10:53 AM
10					

Frequent errors in submission/review of electronic data

Maintain and check the chain of custody of a device

Submission of data in an encrypted media with safe custody of passwords

Device identification and collection procedures during investigating ESI (missing critical devices)

Time zone and Systems date and time information (e.g. BIOS date)

Hash verification post imaging / post analysis of evidence

Electronic chat artefacts missed during investigations

Phone Backups available on investigated devices

Safely seal electronic evidences into safe custody without damaging contents and authenticate the copy of evidence using hash values.