John Doe Hard Drive data analysis and Report

iQwest Information Technologies, Inc. has been engaged to report and analyze contents of the computer hard drive data collected by the Government as a result of property seized at the location of business. The hard drives were produced by the Government with standard DD forensic images of the original. This information was extracted by iQwest into standard file structures according to how they were presented on the drives at the time of collection.

The data was collected for the files visible as well as any deleted files that were not overwritten. For the latter, files only in existence at the time of collection are available for analysis. This means that if any size was required on the drives for new files that contained deleted items, these files would have been deleted at any time prior to the collection and during normal computer usage.

iQwest has separated these two types of collections into separate reports to allow for better reporting and analysis. Every effort has been made to eliminate system files from this collection, although due to the nature of the file extension naming anomalies some system files may have found their way into data being presented. The total size of the file types is minimal and can be further investigated upon data review.

The total data for the data collected is 4.3 Terabytes, of which 972 Gigabytes belong to standard hard drive data and 3.3 Terabytes belong to the unallocated space data. As a result of advanced file type detection technologies we have identified different files by reading the document signature rather just relying on the document extension. This has provided us with the capability to eliminate a large portion of the files being detected. The tools used for the file type detection and extraction are outside the basic scope of this project, although we felt necessary to provide reports of what can be extracted that may be relevant. This has also reduced the total data size dramatically. Additional extraction would be necessary to actually extract this data.

As a result of the file type detection the total potentially relevant data size has been reduced to approximately 150.7 Gigabytes, of which 90.5 Gigabytes is related to standard files (excluding the unallocated space) and 60.2 Gigabytes is related to deleted items being potentially relevant that were detected from the unallocated space.
Also as a result of the file type detection we have identified many of the files that can be eliminated, based on date ranges and decisions made for elimination of additional file types that may not seem as potentially relevant. We will provide this information in the following reports.

Preliminary Forensic Content & Activity Report: Hard Drive Images

Case Intake Information:

Case Matter:	John Doe Acme Manfacturers Ltd.
Project ID:	Doe ESI
Legal Case Info:	Internal Investigation
Individual Requesting Investigation Work:	
Project Description:	Analysis of Government Collected Hard Drives Following an indictment
Report Author:	Pete Afrasiabi, iQwest Information Technologies
Report Date:	Sunday, September 21, 2008

Items Related to Investigation:

Total Item #:	Description:	Custodian:
28	Computer Content from Various Hard drives collected	John Doe

The total data size being reported has been separated into:

1- Standard Drive Data
This section is related to the actual files that appear on the hard drives and as depicted as viewable files on the volumes prior to the collection.

2- Unallocated Space Data
This section references the total size of the volumes that is showing as available storage space per volume. Despite what the term "Unallocated space" depicts there is actual data contained in this space. Any files that are deleted from drives are maintained in this space until the operating system requires more storage space. At this point the operating system will overwrite some of the older deleted items with the needed space for the new ones.

1- Standard Drive Data

As mentioned earlier from the total data size for the standard document collections excluding the unallocated space, we have identified approximately 90.5 Gigabytes that may be potentially relevant. In the following page table 1.1 displays results for each of the identified drives/media/external storage as mentioned in the table provided by the Government. Additional columns display total data size for each folder and shows each as a percentage of the whole collection.

Table 1.1 Volume Distribution

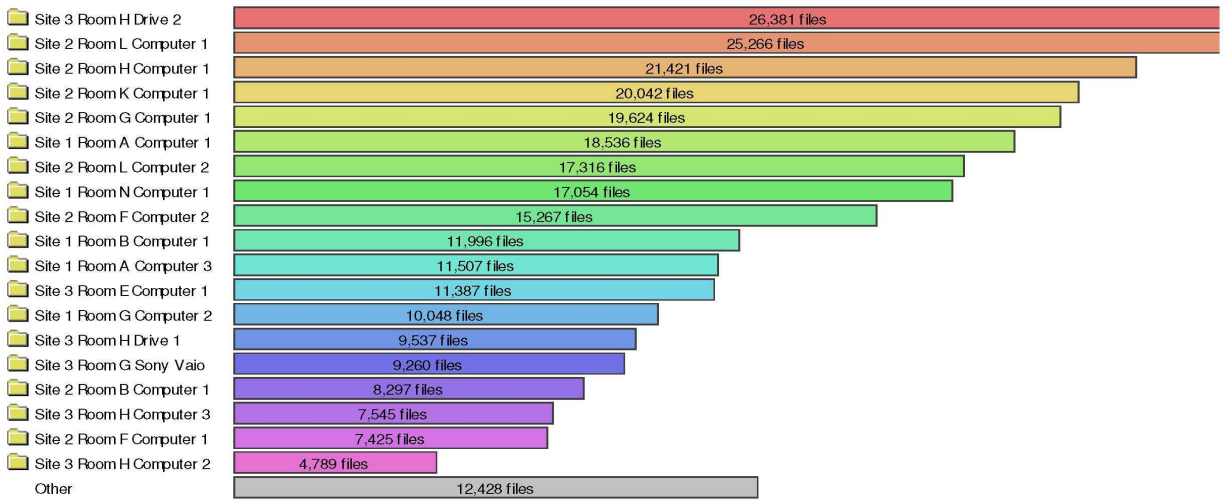
Size details for D:¥HDD-IMAGES

Name	File Size	Files	% of Parent	% of Total
D:¥HDD-IMAGES	94,870,841	285,126	100.00%	100.00%
Site 3 Room H Drive 2	51,432,373	26,381	9.30%	9.30%
Site 2 Room L Computer 1	2,657,164	25,266	8.90%	8.90%
Site 2 Room H Computer 1	741,728	21,421	7.50%	7.50%
Site 2 Room K Computer 1	11,397,229	20,042	7.00%	7.00%
Site 2 Room G Computer 1	1,535,560	19,624	6.90%	6.90%
Site 1 Room A Computer 1	1,611,703	18,536	6.50%	6.50%
Site 2 Room L Computer 2	1,331,366	17,316	6.10%	6.10%
Site 1 Room N Computer 1	709,289	17,054	6.00%	6.00%
Site 2 Room F Computer 2	2,154,765	15,267	5.40%	5.40%
Site 1 Room B Computer 1	403,763	11,996	4.20%	4.20%
Site 1 Room A Computer 3	483,547	11,507	4.00%	4.00%
Site 3 Room E Computer 1	489,510	11,387	4.00%	4.00%
Site 1 Room G Computer 2	3,194,462	10,048	3.50%	3.50%
Site 3 Room H Drive 1	1,302,098	9,537	3.30%	3.30%
Site 3 Room G Sony Vaio	563,227	9,260	3.20%	3.20%
Site 2 Room B Computer 1	1,200,620	8,297	2.90%	2.90%
Site 3 Room H Computer 3	688,112	7,545	2.60%	2.60%
Site 2 Room F Computer 1	817,830	7,425	2.60%	2.60%
Site 3 Room H Computer 2	217,962	4,789	1.70%	1.70%
Site 3 Room H Computer 1	717,413	4,750	1.70%	1.70%
Site 2 Room L Computer 3 Raid 1	10,406,824	3,612	1.30%	1.30%
Site 2 Room C Computer 1	168,834	1,343	0.50%	0.50%
Site 1 Room G Computer 1 Raid0	123,770	1,221	0.40%	0.40%
Site 2 Room B Computer 2 Drive 1	56,009	1,033	0.40%	0.40%
Site 3 Room H Jump Drive 2	271,395	272	0.10%	0.10%
Site 1 Room G Computer 1 Raid1	138,113	177	0.10%	0.10%
Site 3 Room H Jump Drive 1	163	13	0.00%	0.00%
Site 3 Room H Jump Drive 3	56,024	7	0.00%	0.00%

Although the table illustrates the file size of drives and a percentage of each compared to the total, this percentage is vastly different than the file count per volume. This information may assist Counsel to establish trends and usages for the various volumes.

The following illustration depicts this information in a bar chart to allow better understanding of the distribution of data.

Chart 1.1



For a better understanding of the data contained in this collection we have provided some basic charts and reports of the this information based on File type, File size and Last Modified Date.
Notice that in table 1.3 jpg files take up 33.1 percent of the total file size. This file type may be eliminated or redirected and be reviewed in different ways than standard document review mechanisms.

Table 1.2 – File Type Distribution

File types in D:¥HDD-IMAGES-Recovered				
Extension	File Sizes (KB)	% of Total	Files	% of Files
jpg	31,443,113	33.10%	89,731	31.50%
png	924,863	1.00%	60,219	21.10%
htm	737,209	0.80%	53,689	18.80%
html	130,907	0.10%	18,245	6.40%
lnk	15,945	0.00%	14,990	5.30%
pdf	5,989,734	6.30%	7,783	2.70%
<None>	855,590	0.90%	7,077	2.50%
pcx	114,671	0.10%	6,323	2.20%
psd	36,719,409	38.70%	4,384	1.50%
zip	2,740,972	2.90%	3,864	1.40%
ogg	214,371	0.20%	3,006	1.10%
eps	593,637	0.60%	2,647	0.90%
rtf	66,929	0.10%	1,441	0.50%
doc	79,761	0.10%	1,242	0.40%
jar	1,432,873	1.50%	1,124	0.40%
gz	10,859	0.00%	1,093	0.40%
xls	29,722	0.00%	1,077	0.40%
wps	108,628	0.10%	884	0.30%
url	1,207	0.00%	868	0.30%
rif	123,477	0.10%	862	0.30%
tif	5,023,730	5.30%	675	0.20%
ppt	91,199	0.10%	548	0.20%
eml	610,955	0.60%	404	0.10%
mdb	870,680	0.90%	337	0.10%
dot	27,100	0.00%	335	0.10%
qbb	148,719	0.20%	325	0.10%
rar	1,486,327	1.60%	314	0.10%
dbf	3,961	0.00%	256	0.10%
qbw	290,844	0.30%	223	0.10%
wcm	4,059	0.00%	122	0.00%
wpd	5,169	0.00%	104	0.00%
wpt	3,527	0.00%	104	0.00%
efx	2,698	0.00%	103	0.00%
wab	14,545	0.00%	84	0.00%
dbx	503,622	0.50%	83	0.00%
wk4	173	0.00%	72	0.00%
xla	19,213	0.00%	70	0.00%
xlt	16,129	0.00%	63	0.00%
wdb	1,747	0.00%	55	0.00%
pub	3,633	0.00%	46	0.00%
pst	3,155,184	3.30%	42	0.00%
df1	150,025	0.20%	37	0.00%
ps	9,873	0.00%	33	0.00%
sas	234	0.00%	21	0.00%
asd	949	0.00%	17	0.00%
ai	1,883	0.00%	16	0.00%
mny	57,996	0.10%	15	0.00%
cdr	198	0.00%	13	0.00%
wks	204	0.00%	11	0.00%
adp	3,657	0.00%	6	0.00%
fdr	1,560	0.00%	6	0.00%
one	4,008	0.00%	6	0.00%
hcr	2,859	0.00%	4	0.00%
jpeg	20	0.00%	4	0.00%
ldf	2,816	0.00%	3	0.00%
mdf	12,032	0.00%	3	0.00%
php	39	0.00%	3	0.00%
tiff	138	0.00%	3	0.00%
dwg	3,284	0.00%	2	0.00%
lzh	1,024	0.00%	2	0.00%
ppm	385	0.00%	2	0.00%
tar	220	0.00%	2	0.00%
wk1	364	0.00%	1	0.00%
wk3	3	0.00%	1	0.00%
wri	6	0.00%	1	0.00%

The following table displays 50 of the largest files contained in these volumes.

Table 1.3 – 50 Largest Files

50 largest files in D:¥HDD-IMAGES-Recovered			
No.	Name	File Size	Modified
1	Outlook.pst	1.0 GB	Mar 6, 2008 11:48 AM
2	Outlook.pst	618.1 MB	Dec 3, 2007 9:53 AM
3	Outlook.pst	265.5 MB	Mar 6, 2008 7:54 PM
4	Aleanas magnet copy.eps	258.7 MB	Feb 21, 2007 3:24 PM
5	Outlook.pst	238.3 MB	Oct 2, 2007 5:08 PM
6	Inbox.dbx	153.0 MB	Feb 14, 2008 2:15 PM
7	backup.pst	151.1 MB	Nov 21, 2007 1:55 PM
8	backup.pst	151.1 MB	Nov 21, 2007 1:55 PM
9	Outlook2.pst	149.2 MB	Mar 7, 2008 10:20 AM
10	Deleted Items.dbx	143.8 MB	Sep 4, 2007 1:39 PM
11	Outlook1.pst	139.5 MB	Feb 15, 2008 3:00 PM
12	Inbox.dbx	137.8 MB	Mar 6, 2008 12:04 PM
13	Outlook.pst	137.6 MB	Mar 10, 2008 4:40 PM
14	Comprehensive Plan for University Housing Final.pdf	116.0 MB	Jan 18, 2008 9:37 AM
15	Comprehensive Plan for University Housing Final.pdf	116.0 MB	Jan 18, 2008 5:37 PM
16	CC12_tmp.eml	105.7 MB	Feb 14, 2007 5:54 PM
17	HiRiseHandbook.pdf	105.1 MB	Feb 23, 2007 3:58 PM
18	Creative home ownership front done.psd	96.8 MB	May 2, 2005 3:31 PM
19	Creative home ownership front done.psd	96.8 MB	May 2, 2005 3:31 PM
20	Creative home ownership front done.psd	96.8 MB	May 2, 2005 3:31 PM
21	Creative home ownership front done.psd	96.8 MB	May 2, 2005 3:31 PM
22	Creative home ownership front done.psd	96.8 MB	May 2, 2005 3:31 PM
23	Creative home ownership front done.psd	96.8 MB	May 2, 2005 3:31 PM
24	Creative home ownership front done.psd	96.8 MB	May 2, 2005 3:31 PM
25	CCA2_tmp.eml	92.0 MB	Feb 8, 2007 4:18 PM
26	Personal Folders(1).pst	92.0 MB	Jul 11, 2007 12:59 PM
27	Postcard.tif	89.1 MB	Jul 27, 2004 1:21 PM
28	Postcard.tif	89.1 MB	Jul 27, 2004 1:21 PM
29	Postcard.tif	89.1 MB	Jul 27, 2004 1:21 PM
30	Postcard.tif	89.1 MB	Jul 27, 2004 1:21 PM
31	Postcard.tif	89.1 MB	Jul 27, 2004 1:21 PM
32	Postcard.tif	89.1 MB	Jul 27, 2004 1:21 PM
33	Postcard.tif	89.1 MB	Jul 27, 2004 1:21 PM
34	archive.pst	83.3 MB	Mar 6, 2008 11:48 AM
35	View from 7th & Clark #2.zip	77.9 MB	Aug 24, 2006 3:20 PM
36	View from 7th & Clark #2.zip	77.9 MB	Aug 24, 2006 3:20 PM
37	View from 7th & Clark #2.zip	77.9 MB	Aug 24, 2006 3:20 PM
38	View from 7th & Clark #2.zip	77.9 MB	Aug 24, 2006 3:20 PM
39	View from 7th & Clark #2.zip	77.9 MB	Aug 24, 2006 3:20 PM
40	View from 7th & Clark #2.zip	77.9 MB	Aug 24, 2006 3:20 PM
41	Building sign 1 copy.eps	74.4 MB	Jan 5, 2007 3:34 PM
42	Creative home ownership front done.psd	73.1 MB	Jul 28, 2004 4:37 PM
43	Creative home ownership front done.psd	73.1 MB	Jul 28, 2004 4:37 PM
44	Creative home ownership front done.psd	73.1 MB	Jul 28, 2004 4:37 PM
45	Creative home ownership front done.psd	73.1 MB	Jul 28, 2004 4:37 PM
46	Creative home ownership front done.psd	73.1 MB	Jul 28, 2004 4:37 PM
47	Creative home ownership front done.psd	73.1 MB	Jul 28, 2004 4:37 PM
48	Creative home ownership front done.psd	73.1 MB	Jul 28, 2004 4:37 PM
49	Realtor Signs (eve).tif	70.4 MB	Apr 19, 2007 5:43 PM
50	Creative home ownership inside done 2.psd	69.4 MB	Jul 29, 2004 11:39 AM

2–Unallocated Space Data

Files in this space are contained in folders numbered based on a serial number that the operating system assigns at time of deleting and assigning empty space. Within these folders, files also use this serialization technique with most files not displaying any extensions assigned to them. In analysis of the data contained in this space we used advanced file type detection tools to determine whether any of the files contained in this space fall within the allowable and non system file types. This is using this determination to provide files in the following tables and charts to assign the potentially relevant category.

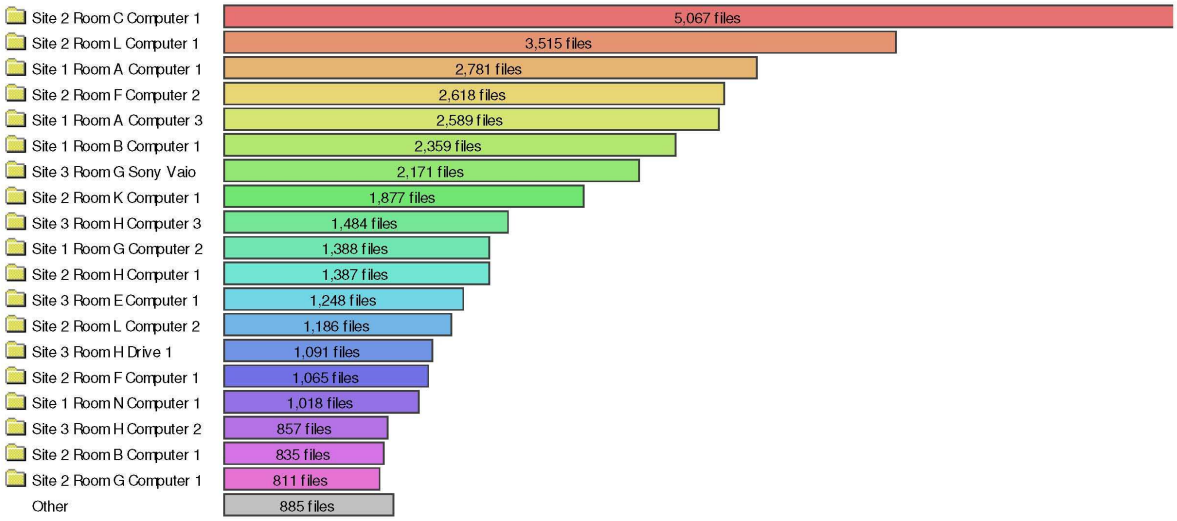
In the following page table 1.4 displays results for each of the identified drives/media/external storage as mentioned in the table provided by the Government. Additional columns display total data size for each folder and shows each as a percentage of the whole.

Table 1.4-Volume Distribution

Size details for D:¥Deleted Files				
Name	File Size	Files	% of Parent	% of Total
D:¥Deleted Files Recovered	63,125,094	36,232	100.00%	100.00%
Site 2 Room C Computer 1	6,041,088	5,067	14.00%	14.00%
Site 2 Room L Computer 1	6,151,404	3,515	9.70%	9.70%
Site 1 Room A Computer 1	8,674,906	2,781	7.70%	7.70%
Site 2 Room F Computer 2	2,729,348	2,618	7.20%	7.20%
Site 1 Room A Computer 3	1,654,036	2,589	7.10%	7.10%
Site 1 Room B Computer 1	2,245,304	2,359	6.50%	6.50%
Site 3 Room G Sony Vaio	970,144	2,171	6.00%	6.00%
Site 2 Room K Computer 1	4,939,420	1,877	5.20%	5.20%
Site 3 Room H Computer 3	2,427,256	1,484	4.10%	4.10%
Site 1 Room G Computer 2	1,150,096	1,388	3.80%	3.80%
Site 2 Room H Computer 1	63,988	1,387	3.80%	3.80%
Site 3 Room E Computer 1	448,188	1,248	3.40%	3.40%
Site 2 Room L Computer 2	5,705,968	1,186	3.30%	3.30%
Site 3 Room H Drive 1	35,596	1,091	3.00%	3.00%
Site 2 Room F Computer 1	226,908	1,065	2.90%	2.90%
Site 1 Room N Computer 1	10,392,700	1,018	2.80%	2.80%
Site 3 Room H Computer 2	569,132	857	2.40%	2.40%
Site 2 Room B Computer 1	1,873,024	835	2.30%	2.30%
Site 2 Room G Computer 1	1,331,300	811	2.20%	2.20%
Site 3 Room H Computer 1	274,904	512	1.40%	1.40%
Site 1 Room G Computer 1 Raid0	254,880	195	0.50%	0.50%
Site 3 Room H Drive 2	4,142,972	75	0.20%	0.20%
Site 2 Room B Computer 2 Drive 1	25,860	47	0.10%	0.10%
Site 2 Room L Computer 3 Raid 1	371,554	47	0.10%	0.10%
Site 2 Room L Memory 1	2,928	5	0.00%	0.00%
Site 3 Room H Jump Drive 3	14,418	2	0.00%	0.00%
Site 2 Room B Computer 2 Drive 2	12	1	0.00%	0.00%
Site 3 Room H Jump Drive 2	407,760	1	0.00%	0.00%

Although the table illustrates the file size of drives and a percentage of each compared to the total, this percentage is vastly different than the file count per volume. This information may assist the Counsel to establish trends and usages for the various volumes.
The following illustration depicts this information in a bar chart to allow for better understanding of the distribution of data.

Chart 1.2



For a better understanding of the data contained in this collection we have provided some basic charts and reports of the this information based on File type, File size and Last Modified Date.
Notice that in table 1.3, jpg files take up 33.1 percent of the total file size. This file type may be eliminated or redirected and be reviewed in different ways than standard document review mechanisms resulting in space occupied.

Table 1.2 – File Type Distribution

File types in D:¥Deleted Files				
Extension	File Sizes (KB)	% of Total	Files	% of Files
jpg	23,173,678	36.70%	15,524	42.80%
htm	7,004,456	11.10%	8,342	23.00%
xml	8,762,456	13.90%	3,705	10.20%
<None>	3,463,000	5.50%	2,669	7.40%
png	4,241,664	6.70%	2,459	6.80%
zip	3,523,916	5.60%	1,160	3.20%
lnk	2,532,540	4.00%	620	1.70%
gz	997,196	1.60%	337	0.90%
pdf	697,912	1.10%	259	0.70%
rar	2,935,704	4.70%	257	0.70%
wmf	17,468	0.00%	161	0.40%
eps	166,012	0.30%	112	0.30%
wav	46,504	0.10%	111	0.30%
psd	2,195,964	3.50%	89	0.20%
eml	196,936	0.30%	80	0.20%
fdr	47,496	0.10%	51	0.10%
doc	26,644	0.00%	48	0.10%
wk3	56,476	0.10%	43	0.10%
tif	1,016,144	1.60%	34	0.10%
rtf	4,080	0.00%	33	0.10%
emf	24,360	0.00%	28	0.10%
dbf	83,012	0.10%	19	0.10%
mdb	13,888	0.00%	14	0.00%
xls	80,664	0.10%	13	0.00%
sas	240	0.00%	12	0.00%
dbx	254,852	0.40%	10	0.00%
ppt	644	0.00%	8	0.00%
db	512	0.00%	7	0.00%
url	246,220	0.40%	6	0.00%
pst	1,034,184	1.60%	5	0.00%
efx	160	0.00%	4	0.00%
qbb	79,932	0.10%	3	0.00%
wps	12	0.00%	3	0.00%
df1	152,832	0.20%	2	0.00%
mny	2,604	0.00%	1	0.00%
pub	31,052	0.00%	1	0.00%
qbw	13,504	0.00%	1	0.00%
wab	176	0.00%	1	0.00%

The following table displays 50 of the largest files contained in these volumes.

Table 1.3 – 50 Largest Files

50 largest files in D:¥Deleted Files Recovered			
No.	Name	File Size	
1	17451766.jpg	1.9	GB
2	10636464.zip	1.6	GB
3	08174392.jpg	1.5	GB
4	29851972.htm	1.3	GB
5	24995851.jpg	1.2	GB
6	36473539.rar	1.1	GB
7	47776424.gz	889.9	MB
8	18381907.png	704.6	MB
9	25054506.xml	694.6	MB
10	16983946.xml	692.8	MB
11	36715314.jpg	632.0	MB
12	18756245.psd	595.4	MB
13	12276241.png	595.2	MB
14	38189723.xml	558.1	MB
15	10276899.jpg	533.7	MB
16	37307336.rar	494.8	MB
17	10168383.jpg	490.6	MB
18	09031132.htm	482.1	MB
19	13190666.pst	452.1	MB
20	10419676.tif	417.8	MB
21	14441850.png	401.8	MB
22	33840775.xml	401.5	MB
23	05749.LNK	398.2	MB
24	43814360.htm	382.8	MB
25	48004268.png	348.6	MB
26	15271815.tif	343.7	MB
27	13583894.xml	342.1	MB
28	44892104.jpg	330.2	MB
29	38782157.jpg	327.5	MB
30	38451406.jpg	317.4	MB
31	14138594.jpg	317.3	MB
32	28373214.png	297.9	MB
33	11980450.pst	293.9	MB
34	36986966	291.3	MB
35	11632105.htm	282.4	MB
36	47360044.jpg	280.3	MB
37	30292277.jpg	273.2	MB
38	18953847.psd	271.3	MB
39	30414115.jpg	257.1	MB
40	14755729.jpg	253.3	MB
41	39721541.jpg	251.9	MB
42	25169940.xml	251.2	MB
43	13682303.png	249.7	MB
44	17073756.dbx	248.0	MB
45	38960511.htm	245.2	MB
46	16106620.pst	241.2	MB
47	29518422.jpg	236.1	MB
48	31801531.url	235.6	MB
49	45173550.jpg	232.8	MB
50	11833476.xml	230.1	MB

Recommended Next Steps:

- Meeting between examiner and counsel to review the complete data contained within the forensic images and discuss next steps and potential options.
- Production of the supporting tables summarized within this report for client review.
- Draft timeline of events relating to notable activities both on the computer and outside events leading up to the time of forensic collection of the data.
- Search for user webmail accounts including regularly visited T-mobile, MSN, Google and Yahoo websites all of which offer web based email accounts.
- Organization of data extracted to allow for better understanding of the nature of data based on various criteria.
- Further production of files, and forensic analysis of relevant data and activities on dates of notable activity.

Conclusion

This report has focused mainly on the overall data sizes and types per volume for this collection. Additional analysis and reporting can be performed on this data based on the needs of counsel and requirements set forth in the future requests. These reports are include but are not limited to the following:

- Registry hive analysis per machine
- Files or programs utilized prior to the date of collection according to the Windows prefetch information contained in this data.
- Internet viewing history information on a per user basis.
- Internet favorites information as shown in the favorites folders.

Depending on the nature of the case and requirements, the data contained in this collection can be separated into small batches according to different criteria and produced according to these requirements.

Further scoping of these requirements is recommended. This can be accomplished with meetings between the investigator and counsel.