Appendix 50 - Process of obtaining electronic server data & PC images

BBY server data obtained from PPB

KPMG Forensic liaised with Rodney McKemmish (PPB) and Mark Monzon (PPB) to collect the server data that PPB, as Receivers and Managers, obtained. PPB advised KPMG that PPB was unable to retrieve an independently verifiable forensic image of the server, due to restrictions on being able to obtain physical access to the server data. PPB advised KPMG that they downloaded the contents of the server via an internet connection. PPB advised that this was the best available option to obtain the data due to the restrictions imposed, however acknowledged that this is not forensically verifiable method of data capture.

On 10 June 2015 KPMG provided PPB three six terabyte Western Digital hard drives for PPB to transfer the BBY server data on to. On 9 July 2015 Mark Monzon returned the three six terabyte Western Digital hard drives to KPMG, two of which were used to store the BBY server data. The third Western Digital hard drive was not required. The two hard drives consisted of compressed AccessData image files (.ad1). The data on the drives, in its compressed state totalled approximately 6.54 TB. In its uncompressed form, the size of the data would represent a much larger volume (potentially up to 10TB+).

Since KPMG Forensic have obtained this data, KPMG Forensic have stored the data in the secured Forensic Labs in Sydney and Perth.

Forensic Computer Imaging - Sydney

Onsite computer imaging was completed by KPMG Forensic on the 26th and 27th May 2015. A total of 13 independently verifiable forensic images were captured from computer hard drives. The computer hard drives to be forensically imaged were selected based on a list of custodians selected by KPMG Forensic and KPMG Restructuring. Jerry Sarantis (BBY - Infrastructure Support Engineer) and Jane Quinn (BBY) assisted in the identification of the physical location of the relevant custodians' PC.

Once identified, the PCs (including asset numbers and serial numbers) were photographed in their original location prior to being powered down and unplugged from all peripheral connections. Computers were then transported to an on-site room provided to KPMG Forensic for imaging. This on-site room was locked when the room was left unattended by KPMG Forensic staff without fail.

The following procedure was used to forensically image the PC hard drives:

1) Remove the side door of the physical PC casing
2) Disconnect the power cable(s) and SATA cable(s) connecting both the computer hard drive **(Source Drive)** and the DVD drive
3) Connect a KPMG Hard Drive (NTFS formatted SATA Hard Drive – Western Digital 6TB or 4TB) **(Evidence Drive)** to the power cable and SATA cable previously used for the DVD drive
4) Connect USB external DVD drive containing KPMG Forensic Technology Linux Boot Disk to the PC's USB port
5) Connect KPMG USB keyboard
6) Power on the PC and confirm the required keyboard input to select boot menu
7) Power off the PC
8) Re-connect the power cable and SATA cable to the Source Drive
9) Power on the PC and select boot menu
10) Boot from external DVD drive (KPMG Forensic Technology Linux Boot Disk)
11) Input KPMG case information and source drive information (e.g. custodian, job number, job name, location, image name etc.)
12) Image drive to a raw DD image or .e01 image
13) Verify image (automatic)
14) Check verification was successful
15) Power off PC
16) Remove Evidence Drive
17) Restore all connections on the PC (e.g. DVD drive)
18) Restore the side door onto the PC and return it to its original location.

The following computers from the identified custodians were forensically imaged:

Asset ID	Hard Drive Capacity (approximate)
BBYSYDDSK150	500 GB
BBYSYDDSK208	1000 GB
BBYSYDDSK123	250 GB
BBYSYDDSK64	500 GB
BBYSYDDSK214	500 GB
BBYSYDDSK195	1000 GB
BBYSYDDSK57	160 GB
BBYSYDDSK333	250 GB
BBYSYDDSK250	1000 GB
BBYSYDDSK263	500 GB
BBYSYDDSK59	160 GB
BBYSYDDSK122	250 GB
BBYSYDDSK338	500 GB

The independently verifiable forensic images were then bought back to the KPMG Forensic Lab. Raw .DD images files were then compressed into .e01 files using X-Ways. E.01 files were then verified using cryptographic hashes to match the original evidence.

Forensic Computer and Phone Imaging - Melbourne

Computer Imaging was completed by KPMG Forensic on the 13th and 27th May 2015.

A total of 4 independently verifiable forensic images were capture from computer hard drives. 3 independently verifiable forensic images were created and verified using AccessData FTK Imager. 1 independently verifiable forensic images were created and verified using EnCase v7.08.

The following PC from the identified custodians were forensically imaged:

Asset ID	Hard Drive Capacity (approximate)
BBYMELDSK13	240 GB
BBYMELDSK60	240 GB
BBYMELDSK02	80 GB
BBYMELDSK69	240 GB

A total of 1 independently verifiable forensic image was captured from a BlackBerry 8110 mobile phone.

Mobile IEMI
357564.02.601073.0

Following the imaging process, all data was retained within the secured KPMG Forensic Technology Labs in Sydney, Melbourne or Perth. If hard drives were required to be mailed between offices, they were sealed with Forensic tape and verified on arrival prior to be utilised for analysis.

Email review

Email data from the independently verifiable forensic computer images was indexed and relevant search terms run over the data. The results of these search terms were then exported and reviewed on an internal e-discovery platform. Searches were conducted over 57,351 individual email items which were extracted from the forensic computer images.

Email data from the BBY server data was processed per custodian mailbox. A total of 2,787,560 individual email communication items were identified from a list of relevant custodians and functional mailboxes selected by KPMG. Search terms were run over this data to identify relevant email communications and documentation.

Additionally, scoped searches were conducted on specific custodian email mailboxes. These mailboxes were exported and reviewed separately on an internal e-discovery platform. The volume of items searched on the e-discovery platform per custodian was:

Cases	Range	Total Items	Total Emails (deduplicated)
1	All Dates	517,007	178,653
2	Pre 2015	1,029,171	360,790
3	2011/12/13/14	283,311	94,636
4	2013/14/15	202,429	72,505
5	All data before 31 Dec 2014	283,311	98,065
6	All Dates	8254	238
7	All Dates	147,242	46,144
8	All Dates	170,686	62,932
9	All Dates	261,235	109,286
10	All Dates	625,632	247,781
11	All Dates	68,888	28,029
12	2013/14	183,761	68,328