Digital response services

Advanced Mobile Device Data Recovery

Locked out of your damaged device? Know how you can recover.

It can happen to anyone.
When a senior level executive recently mistakenly dropped his mobile device while getting into a car, accidentally driving over it, causing significant damage to the screen, keypad, and data connections. Efforts were made to repair the device, but it remained inoperable.

All was not lost, however, as KPMG Cyber professionals came to the rescue. They were able to successfully remove the flash memory from the device and complete a full data recovery. What seemed like a potential nightmare turned out to be a positive outcome: the executive's sensitive data was recovered and then securely provided back to the client.

Today's reality

- Mobile devices have become heavily intertwined into everyday business and life—with personal devices containing work material and vice versa.
- The acquisition of data from mobile devices presents a number of limitations for accessing deleted data. Oftentimes damaged device examinations are impossible when using traditional forensic approaches.
- As device security has been increased, unlocking a device may be impossible without knowledge of the user's password, fingerprint, or other security implementation. Detailed analysis and data recovery may require more time and effort than ever before, and the inability to access the data only exacerbates these issues.

Seventy-two percent of employees store sensitive data on their mobile device.[1] As mobile devices become more prevalent in the marketplace, they also become more interconnected and contain the potential to store even greater volumes of vital data. Often the ability to acquire data from a device is limited to a software application's ability to interface with it. In the event of a physically damaged or a locked device, the ability to acquire the data through conventional retrieval methods may be impossible.

[1] Fujitsu Mobile Workplace Device Management

Example use cases:

- A device is physically damaged by water or fire beyond repair
- An employee has intentionally or unintentionally damaged or lost the password to unlock the device
- A Device Operating System is restricting access to user data (e.g., Blackberry devices, Windows phones or locked boot loader Android devices)
- Data recovery is needed from damaged USB flash media
- A traditional software application will not acquire a full bit stream image of a device (which is needed to recover deleted data)

Recovery methods

For these cases, the ability to complete a **JTAG** (Joint Test Access Group) bypass acquisition, an **ISP** (Inline Service Programming) bypass acquisition, or a binary flash memory **Chip-Off** extraction may be among the only ways to access the physical image of the device. The type of device is the driving factor for the method of recovery. The options vary from minimally invasive/non-destructive to a destructive process:

JTAG (Joint Test Action Group)

JTAG is a non-destructive process of retrieving data from an intact or semi-intact mobile device. JTAG provides a bit stream image of the internal memory storage through a manufacturer-installed test access point. When the process is complete, the device is fully functional with no physical damage.

ISP (Inline Service Programming)

Similar to JTAG, Inline service programming (ISP) results in a bit stream image of the memory chip in the device through another hardware mechanism associated with an embedded MultiMediaCard (eMMC). ISP is also a non-destructive collection process. After completed, the device remains fully functional with no physical damage.

Chip-off

Chip-off is a destructive process and involves the removal of the device's memory chip, and then a bit stream image is obtained. (This would be the equivalent of removing a hard drive from a computer to obtain a forensic image for analysis.) This process is not limited to mobile devices alone, and can be applied to USB flash media and solid state drives. A similar process can be applied to monolithic Micro SD cards. This is the ideal solution when a device has been damaged beyond repair, or JTAG/ISP is not available.

- There are two types of flash memory chip technology—NAND Flash and eMMC/eMCP Flash memory. NAND requires an external controller to recover data from the flash memory. This results in the need for a special adapter.
- The process requires access to special electronic rework equipment, chip program readers, and skills to remove, clean, and recover data from the embedded memory chip. While all necessary precautions are exercised, this extraction methodology could result in damage to the memory chip and will render the device inoperable.

While Chip-off, JTAG, and ISP are not operating system-dependent, there are hardware limitations. Devices which implement hardware or software encryption may result in limited data recovery. By the same token, these devices typically have limited data recovery in a live and unlocked state. Additionally, encryption may prevent the recovery of user data.

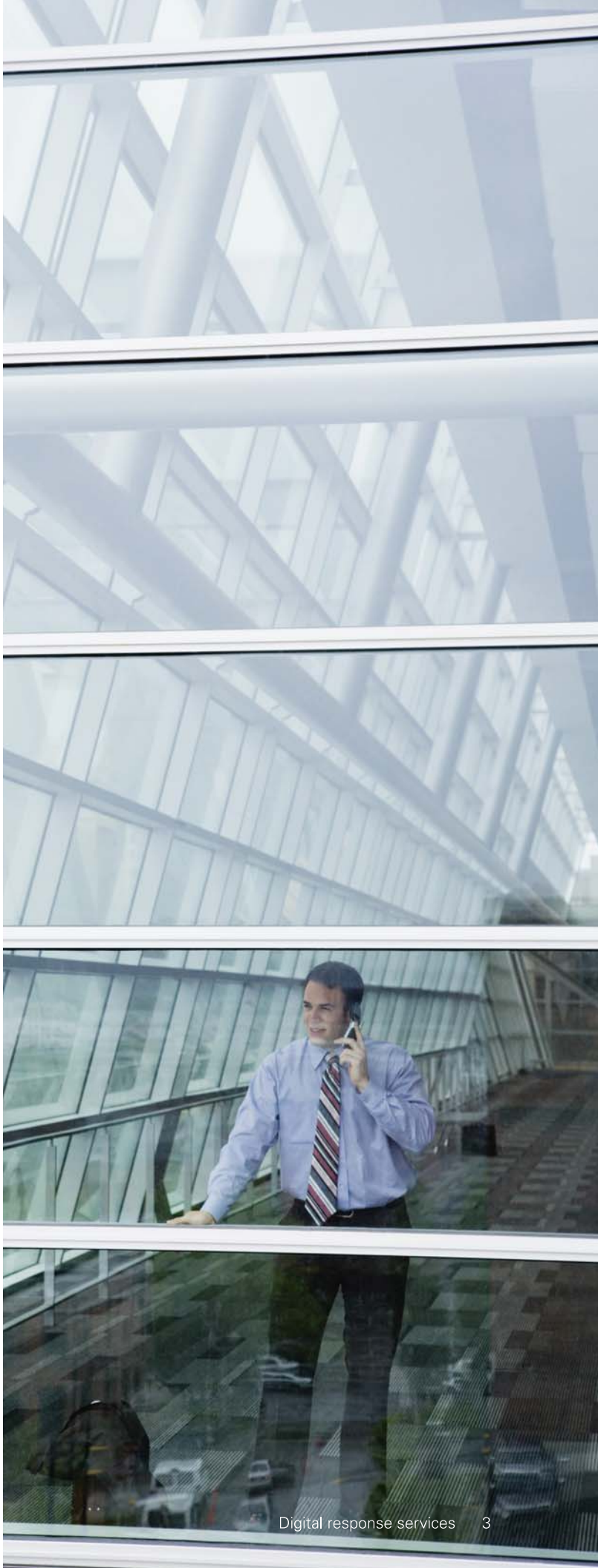
KPMG

Three phases of data recovery

1. **Assessment Phase:** The assessment phase of data recovery consists of the identification of the device and internal flash memory. All possible data recovery methods are identified and recommendations are made. While a device may be physically damaged, repairing the device instead of completing a Chip-off may be the appropriate course of action. If Chip-off extraction is determined to be the best course of action, all other collection methods are attempted prior to completing the Chip-off process. A test device of the same make and model may be purchased, and the methodology would be validated prior to completing the process on the evidence device.
2. **Acquisition Phase:** The acquisition phase involves the disassembly of the device, and from there, either the removal of the embedded flash memory chip or data access via identified access points. If the memory chip is removed, it is cleaned and new ball grid array (BGA) solder is applied to the underside of the chip and a copy is created.
3. **Analysis Phase:** Recovery from flash memory presents many challenges such as multiple files system, proprietary operating system, and non-contiguous data structures. Like traditional hard drives, data is stored in organizational structures; however, due to the difference between traditional hard disk storage and flash media structure, data recovery methods and the end result may vary. After the data has been recovered from the memory chip, a variety of traditional forensic tools and methods can be utilized to analyze data and provide valuable findings.

Support device platforms

Blackberry, Windows Phone, Android, Symbian, Feature Phones, GPS Units, USB Flash Media



About KPMG's Digital Response Services

KPMG member firms employ over 2,500 cyber professionals globally who are available to help you with your cyber needs. Many of these professionals are leaders in the cyber community, helping to develop the tools and methodologies used to combat cybercrime on a daily basis.

Our professionals have experience working on a variety of cybercrimes, including insider threats, data breaches, hacktivism, and advanced persistent threat-style intrusions by highly motivated adversaries. Our services include a variety of strategy and investigation offerings to support your needs.

KPMG is also heavily involved in the information security community. This involvement provides us with early insight into emerging issues, which we share with our clients and our project support teams, as a component of our advisory role. The pragmatic advice and the services we can offer your organization are shaped from the experience we have gained and relationships we have developed serving clients of various size, scope, and complexity.

About KPMG Cyber

Keep it simple—the right balance of information protection and accessibility.

The KPMG Cyber approach is designed to be simple and effective, and most importantly, aligned with the business needs of our clients. KPMG Cyber assists global organizations in transforming their security, privacy, and continuity controls into business-enabling platforms, while maintaining the confidentiality, integrity, and availability of critical business functions.

For more information, contact us:

Edward Goings
Principal, KPMG Cyber –
Digital Response Services Lead
T: 312-665-2551
E: egoings@kpmg.com

David Nides
Director, KPMG Cyber
T: 312-665-3760
E: dnides@kpmg.com

KPMG Cyber Emergengy Hotline at 855-444-0087

kpmg.com/us/cyber

kpmg.com/socialmedia