INFORMATION SHEET PASSWORD RECOVERY

DISCLOSING PROTECTED DATA...

APPLICATIONS
- Salvaging and / or disclosing data protected by unknown passwords or cryptographic controls.
- Business continuity.
- Data loss prevention.
- Removing malware enabled encryption on infected storage media.
- Preparing evidence for litigation support.
- Fact-finding investigations.
- Investigate data loss and compromises.
- Asset recovery investigations
- Safeguarding an organizations considerable interests.

INTENDED FOR
- Law firms and solicitors.
- Financial institutions.
- Insurance companies.
- Corporate sector and industry.
- Investigative companies.
- Government agencies.

Password Recovery - Cryptanalysis - Decryption
The ever increasing amount of data being protected through passwords and encryption, also implies a substantial increase in data loss because of lost passwords. And with the use of strong cryptographic products and multi factor authentication on the rise as well, disclosing protected data becomes more and more difficult when credentials or cryptographic keys are lost.

The human factor vulnerability
Besides lost or forgotten passwords, what about the disgruntled (former) employee that simply refuses to hand over the credentials used for securing confidential company data? This becomes particularly problematic with biometric security measures in place. From a legal perspective it is not easy to enforce a current or former employee to provide his or her fingerprints for data disclosure.

Cryptanalysis and Decryption
Nowadays, passwords stored on computer systems are not kept in plain text, but rather as so called hashed values. These are the result of irreversible cryptographic algorithms that protect the actual password from being compromised.

Cryptanalysis and decryption refers to the analysis of protected data in order to identify weaknesses that will enable disclosure of that data without necessarily knowing the key or the algorithm.

Recovery and resetting of passwords
As most, if not all security measures and controls have weaknesses, fortunately the majority of passwords can be recovered or reset within a reasonable timeframe. Depending on the strength of the applied security, passwords can sometimes even be recovered or reset instantly. On the other side of the complexity spectrum, when extremely strong cryptographic controls are utilized, data can sometimes only be disclosed by brute forcing methodology. This adds substantial time to the disclosure process, while some security controls are so strong it might even take years or indefinite to disclose the data concerned.

Xandstorm provides password recovery and decryption services covering more than 200 individual file types. Utilizing hardware accelerated computing and a distributed network of dedicated decryption nodes, we are able to disclose data that was thought to be lost for ever.