

best practices

by Best Practices Best Pracices

Submission date: 05-Feb-2019 01:37PM (UTC-0700)

Submission ID: 1073541609

File name: best_practices_final_33.pptx (1.32M)

Word count: 1069

Character count: 2936

The background of the slide features an abstract design composed of various shades of blue. On the right side, there are several overlapping, semi-transparent geometric shapes, including triangles and polygons, in different tones of blue, ranging from light sky blue to deep navy blue. These shapes create a dynamic, layered effect. The rest of the background is a solid, very light blue color.

Information security.

Best Practices in Collecting Digital Evidence For DigiFirm Investigation Company.

Introduction.

- Digital evidence refers to information and data which are of value to an investigation carried out through electronic devices (Quick & Choo, 2018).
- Digital evidence can be acquired when an electronic device is seized and secured for examination.
- Evidence handling has been growing due to the expanding field of computer forensics.
- Digital devices have been deemed necessary for addressing the needs of the rapidly changing computing settings (Quick & Choo, 2018).

Rules of Digital Evidence.

- Admissible.
- Authentic.
- Complete.
- Reliable.
- Believable (Quick & Choo, 2018).



THE TRAIL OF
DIGITAL
EVIDENCE
THAT YOU LEAVE BEHIND

Best practice for the forensic investigation life cycle.

- Requirement analysis.
- Definition of all evidence pieces.
- Retrieval of data (Ashley, 2017).
- Reliability.
- Critical focus on the investigation process.
- Critical scrutiny of servers.
- DigiFirm should underscore all these practices.



Continuation of best practice for the forensic investigation life cycle.

- Review of the evidence.
- Representation of evidence.
- Repository of data (Gill & Phythian, 2018).
- Evidence Extraction.
- Forensic tools should be used effectively.

The Best practices in collection of digital evidence.

- Avoid touching the crime gadgets not unless you are required by digital forensics.
- Documentation of the location and conditions of gadgets before handling them professionally.
- Record the manufacturer type and serial numbers of the device (Ashley, 2017).
- In all data transferred, there should recording of date, time , personnel as well as purpose.
- The evidence should be stored in a secure place for security purposes.



Recommendations for the Digifirm.

- DigiFirm should consider performing regular backups (Ashley, 2017).
- Critical scrutiny and auditing should be carried on all the workstations, servers, and network devices.
- In addition, all the audit records should be audited to checked on their security and centralization.
- DigiFirm should maintain its files and databases for critical integrity checking.

Recommendations continued.....

- DigiFirm should focus on conducting computer and network forensics in order to instill critical security.
- DigiFirm should set specific parties for handling different forensic aspects
- All the incident handling teams must prove their prowess in forensic aspects (Ashley, 2017).
- Multiple teams should be granted different roles in forensic evaluation for reliability and validity.
- Diverse policies should be set for addressing forensic handling.
- DigiFirm should set effective, reliable, sustainable and efficient forensic guidelines and procedures.



Conclusion.

- Evidence handling has been growing with the field of computer forensics.
- In this case, DigiFirm should dive deeper into the collection of forensic data.
- The firm should address its forensic considerations through key policies.
- The firm's activities should be complemented with the guidelines and procedures for the improved performance of investigations

References.

Ashley, K. D. (2017). *Artificial intelligence and Modern legal analytics*. Cambridge University Press.

Gill, P., & Phythian, M. (2018). *The Application of Artificial Intelligence in Modern World*. John Wiley & Sons.

Quick, D., & Choo, K. K. R. (2018). Digital forensic Investigation and Intelligence: *Future Computer Systems Generation* 78, 558-567.

best practices

ORIGINALITY REPORT

0%

SIMILARITY INDEX

0%

INTERNET SOURCES

0%

PUBLICATIONS

0%

STUDENT PAPERS

PRIMARY SOURCES

Exclude quotes

Off

Exclude matches

Off

Exclude bibliography

Off