

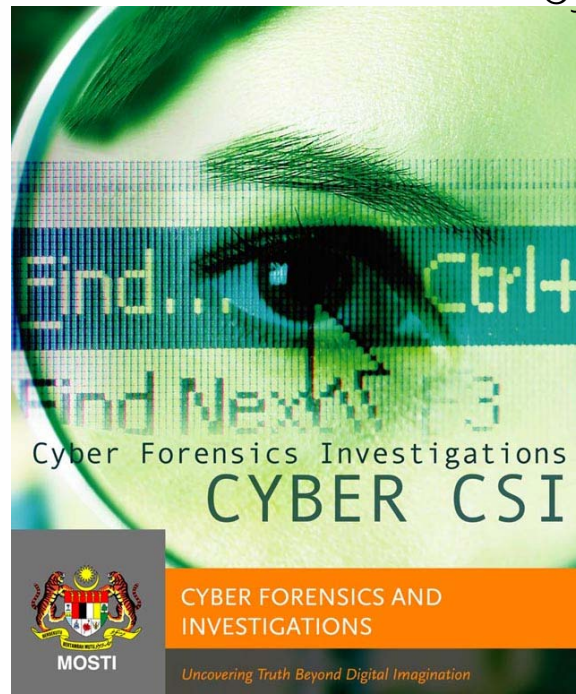


EXPERT WITNESS: Completion of a perfect circle

Cyber Forensics Workshop, Doha, Qatar

February 21, 2008

By R.Azrina R.Othman
CyberSecurity Malaysia



Contents

- About Digital Forensics
- Legal standing
- Preparation
- In Court
- Post mortem
- Conclusion



Digital Forensics Services



**DIGITAL FORENSICS
LAB**
Analyze & Investigate
Digital Evidence



**DATA RECOVERY
LAB**
Recover Corrupted
& Deleted Data



**EXPERT DEVELOPMENT
LAB**
Platform for
Research & Job Attachment



**EVIDENCE PRESERVATION
FACILITY**
A Secured Environment for
Digital Evidence



Contents

- About Digital Forensics
- Legal standing
- Preparation
- In Court
- Post mortem
- Conclusion



Expert witness testimony

- ❑ The end destination of a digital forensics analyst. Completing the full circle of the digital investigation.

- ❑ “Life and death” moment:
 - ❑ If accepted, you are the HERO!.
 - ❑ Otherwise,
 - ❑ Organization’s reputation tarnished
 - ❑ All the hard work went to the drain
 - ❑ May affect your career as digital forensic analyst



Legal standing of Digital Forensic Analyst (1)

❑ Admittance of expert evidence based on Criminal Procedure Code 399

- ❑ Pros – Analyst do not need to provide detail credentials in court as the organization has been gazetted.
- ❑ Cons – The defense counsel will request for time to understand the report and prepare for cross examination.



Legal standing of Digital Forensics Analyst (2)

- ❑ **Acceptance of expert opinion under the Section 5 of The Malaysia Evidence Act 1950**
 - ❑ Pros – The testimony and analysis on the digital evidence will be accepted by court IF the analyst credibility is established.
 - ❑ Cons – The analyst must justify credentials through declaration of qualifications, background and experiences to assure the integrity of the findings and analysis made.



Contents Outline

- About Digital Forensics
- Legal standing
- Preparation
- In Court
- Post mortem
- Conclusion



When the preparation begins

- Court preparation begins upon report completion and submission to law enforcement.

- When a subpoena issued to analyst by law enforcement (LE).

- When statement has been taken by law enforcement officer.



Understanding the facts

- Validate again all findings to ensure the accuracy of facts.
- Ability to demonstrate good technology knowledge relevant to the case
- Firm understanding of how the technology been used to commit the crime.



Understanding the facts

- ❑ Analyst need to understand the whole case-scenario especially on the prosecution matters.
 - How the offense was committed?.
 - How the digital evidence contribute to the case?.

- ❑ Understanding the prosecution matters will build confidence.

- ❑ Seek clarification from Deputy Public Prosecutor (DPP) when in doubt of court procedures.



Statement taking

- Avoid technical details

- Make it as layman as possible and clarity in explaining how technology was used in committing the crime.

- Ensure all key evidences are highlighted

- The statement must be impartial and conclusive.



Contents Outline

- About Digital Forensics
- Legal standing
- Preparation
- In Court**
- Post mortem
- Conclusion



Presentation style

- ❑ Various types of presentation approach to illustrate the findings:
 - Demonstration
 - Animation
 - Slide
 - Verbal / Written report



Presentation of Findings

	Pros	Cons
Demonstration	<ul style="list-style-type: none"> • Will provide better understanding in court 	<ul style="list-style-type: none"> • In uncontrolled environment (court), anything can happen eg. Equipment malfunction, software corrupted, insufficient equipments and etc
Animation	<ul style="list-style-type: none"> • Will provide visual illustration • Suitable for complicated case 	<ul style="list-style-type: none"> • Animation cost is expensive
Slide	<ul style="list-style-type: none"> • Will provide some form of visual reference in court • Defense counsel may find it hard to digest the information for the cross-examination session 	<ul style="list-style-type: none"> • Must have good presentation strategy to ensure the message understood
Verbal / report	<ul style="list-style-type: none"> • Defense counsel may not have any reference for the cross-examination session • Provide high confidence / credits to the analyst 	<ul style="list-style-type: none"> • Focus and avoid mistakes • Need to memorize a lot of details and to ensure accuracy.



Cross-examination session

- Expect manipulated/trap questions from defense counsel with intent to confuse or to make analyst give desirable answers.**
- Maintain consistency in response.**
- Need to be mentally calm and focus.**



Court testimonial: Key Success Factors

1) Credibility of the analyst

Highlight credentials, qualifications and experience.

2) Integrity of Evidence

Chain of custody of the digital evidences maintained and report the findings as it is.

3) Convincing Answers

Give clear and convincing answers. Remain calm and focus esp. during cross examination. Speak slowly, since the court needs to take it down.

4) Conclusive Answers

Avoid any hesitation when answering the prosecution or defense counsel. Answers must be conclusive.



Contents Outline

- About Digital Forensics
- Legal standing
- Preparation
- In Court
- Post mortem
- Conclusion



Post-mortem analysis

- ❑ A post-mortem analysis of an expert witness testimonial should be conducted to analyze court proceedings.
- ❑ Important to obtain feedback from prosecution counsel.
- ❑ Follow development of the court proceeding to determine acceptance of evidence.



Contents Outline

- About Digital Forensics
- Legal standing
- Preparation
- In Court
- Post mortem
- Conclusion



Conclusion

- ❑ Very important to be objective in giving answers in court.
- ❑ Clear goal, which is to have the testimony with regard to the analyzed digital evidence accepted by the court.
- ❑ Prosecution strategy and plan are key contributors.



Our Corporate Website:


 <http://www.cybersecurity.org.my/>


An agency under:



Ministry of Science, Technology & Innovation


[Home](#) > [About Us](#) > **Contact Information**

 **Postal Address** : CyberSecurity Malaysia (formerly known as NISER),
Level 7, SAPURA @ MINES,
7, Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan,
Selangor Darul Ehsan,
Malaysia.

 **Office Hours** : Monday - Friday 08:30 - 17:30 MYT
(Note: Not operational every Saturday and Sunday)

 **Phone** : +603 - 8992 6888

 **Fax** : +603 - 8945 3205

 **Email** : [info \[at\] cybersecurity.org.my](mailto:info@cybersecurity.org.my)

 **Map** : [Click here to download CyberSecurity Malaysia location map.](#)

Thank You!