

Challenges to Digital Forensic Evidence

Table of Contents

1 Introduction and background.....	5
A good background.....	6
Questions.....	7
2 Overview.....	8
Basics.....	8
Faults and Failures.....	9
Legal Issues.....	9
The Latent Nature of Evidence.....	10
Notions Underlying "Good Practice".....	10
The nature of legal systems and refuting challenges.....	11
Overview.....	11
Identifying Evidence.....	11
Common Misses.....	12
Information not sought.....	12
False evidence.....	13
Non-stored transient Information.....	13
Good practice	14
Evidence Collection.....	14
Establishing Presence.....	15
Chain of custody.....	15
How the evidence was created.....	15
Typical Audit Trails.....	16
Consistency of Evidence.....	16
Proper Handling During Collection.....	16
Selective collection and presentation.....	17
Forensic imaging.....	18
Non-Stored Transient Information.....	19
Secret science and countermeasures.....	21
Seizure errors.....	22
Warrant scope excess.....	22
Acting for law enforcement	23
Wiretap limitations and Title 3.....	23
Detecting alteration.....	24
Collection limits.....	25

Challenges to Digital Forensic Evidence

Good practice	25
Fault type review.....	27
Transport of evidence.....	27
Possession and chain of custody.....	27
Packaging for transport.....	27
Due care takes time	28
Good practice	28
Storage of evidence.....	28
Decay with time	29
Evidence of integrity	29
Principles of best practices.....	30
Evidence analysis.....	30
Content.....	31
Contextual information.....	31
Meaning.....	32
Process elements.....	33
Relationships.....	33
Ordering or timing.....	34
Location.....	35
Inadequate expertise.....	36
Unreliable sources.....	36
Simulated reconstruction.....	37
Reconstructing elements of digital crime scenes.....	38
Good practice in analysis.....	40
The process of elimination.....	40
The scientific method.....	41
The Daubert guidelines.....	41
Digital data is only a part of the overall picture.....	43
Just because a computer says so.....	45
Overall summary.....	45
Questions.....	46
3 Mechanics of writing expert rebuttals.....	48
An outline of a report.....	48
In the first person.....	50
Time is of the essence.....	52
We all make mistakes – don't compound them.....	53
Hedge in an honest way.....	54

Challenges to Digital Forensic Evidence

Present the basis with the conclusions.....	56
Do simple experiments to disprove things.....	57
The report is the draft I am working on.....	59
Use analogies within limits.....	61
Why should the standard be lower?.....	62
When in doubt, check it out.....	64
Questions.....	65
4 Case studies.....	67
Don't forget the effects of time.....	69
The WayBack Machine and friends.....	72
Calibrating your own tools.....	73
Issues related to link analysis.....	75
Internet operations between companies.....	80
Malicious exploitation of computers.....	88
The single actor theory.....	91
An early case involving audit trails.....	93
The case of the video of the case.....	105
Mock trial and the MD5.....	108
The virus ate my case.....	109
Spoliation of evidence and chain of custody.....	110
Questions.....	113
5 Testifying.....	115
Prepare.....	116
Tell the simple truth as you know it.....	117
Don't stretch it - be open.....	118
Take your time and think.....	119
Questions.....	120
6 How to avoid being challenged.....	122
Questions.....	124
Index.....	125