Mag. iur. Dr. techn. Michael Sonntag

Expertises: Reading, Writing & Assessing them

Computer forensics

Institute for Information Processing and
Microprocessor Technology (FIM)
Johannes Kepler University Linz, Austria

E-Mail: sonntag@fim.uni-linz.ac.at
http://www.fim.uni-linz.ac.at/staff/sonntag.htm

Agenda

- Anatomy of an expertise
  - → Introduction, glossary etc.
  - → Facts & discovery procedure
  - → Method of evaluation and results
  - → Conclusions
- Tips to look out for
- Expertise's and courts

What is an “expertise”?

- Expertise = Discovery of important facts and/or drawing conclusions from facts
  - → Both are intended to help others which cannot do this themselves
  - → Typically used in connection with a legal action
- Two main types:
  - → Court: The court itself wants to know the real facts
    - » Not what the parties tell it
    - » Additionally: Provide the court with information on what typically follows from certain fact/actions/… (experience)
  - → Private: Someone wants to provide a counter-expertise to the court, or as preparation for court proceedings
  - → Scientific expertise: Something different!
    - » Main issue is here the discovery of something new
    - » This is typically NOT interesting for coud/private expertises (→ proven and generally accepted!)

Why do we need an expert for this?

- Source of information:
  - → Neither court nor parties know perhaps anything about it
- Source of explanations:
  - → Explaining complex situations or reasons for laymen
- Source of reasons: Why did this happen?
- Legitimacy:
  - → Independent, objective, impartial
  - → We have to trust someone, so he/she should live from something else (no interest in being expert), not involved in this conflict (no interest in outcome) and not deciding
- Biggest problem: At the experts mercy
  - → Nobody knows anything
  - → A “god” sends the decision from “heaven”
    - » You just have to trust in the correctness
    - » Which might be very difficult if you lost!

Anatomy of an expertise

- An expertise is almost always a written expertise
  - → Which might be required to be expanded on orally in court, where questions regarding it are possible too
    - » There the curriculum vitae of the expert might be questioned
  - → Oral expertises should (ideally) follow the same pattern!
- Overall structure:
  - → General information: Who has requested the expertise, file number, date, …
  - → Title and topic: What was to do
  - → Surrounding activities: What do the parties agree upon
  - → Findings of fact: What was measured in which way
  - → Conclusions: Fact + laws of nature/experience = ???
  - → Summary: The result without any facts, reasons etc.
  - → Signature: Date, signature, stamp
- Separate: Invoice

Front matter

- General information: Who has requested the expertise, file number, date, …
- Title: General summary of the main point
- Topic: What were the exact questions to the expert?
  - → Courts should ideally provide exactly worded and very specific questions
    - » E.g. “Did person A copy file ‘abc.txt’ on enclosed USB stick?”
    - » Practice (at least sometimes): “Expertise on all relevant matters”
  - → Private expertise: Exact description of what was to do
  - → Note: This is important for possible liability
    - » Only in exceptional cases should there be anything in the expertise, which was not asked for explicitly
      - – Example: Hidden problem potentially very important for the outcome, but which nobody suspected to be there
  - → Should explicitly include whether only facts, only conclusions or facts **and** conclusions were asked for

Facts and discovery procedure

- Discovery procedure: Exact specification of
  - → When, where, who did the measurement
    - » Typically all parties should be present or they must at least be offered the possibility if done at one parties premises
  - → How was the measurement performed
    - » What other methods do exist, why was this one chosen
  - → How "good" is the measurement
    - » Margin of error: Accuracy possible (typically as range)
    - » What can be detected in this way **and what not**
      - – Often forgotten: The limits of the methods employed!
    - » Example: Looking for the string "€ 1000" in all files
      - – ASCII vs. UTF-16? "EUR 1000"? "€ 1.000"? Deleted files? …
- Facts discovered: What was found (and what not)
  - → Specify exactly and only what was found
    - » No conclusions here
    - » No "generally this would also be here"

Facts and discovery procedure

- Describe how you validated the result
  - I.e., what was/should have been there but was (not) found
- No conclusions: Only and solely what was actually "measured" in some way
  - "The following bytes were found in sector xyz: AABBCCDD"
  - "A deleted image showing 'qwertz' was found"
  - Not: "A delete image of child pornography was found"
    - Whether this is child pornography or not is for the court to decide!
- State clearly if something could not be measured
  - "There is not enough data to show whether this took place"
  - Still useful for the judge: Rules of evidence!
- Do not search for additional things
  - This might in extreme cases be criminal behaviour
    - An expert is not the police; he/she should look for clearly defined elements **only**
  - If unavoidable to notice, briefly mention them

Method of evaluation and results

- How did the evaluation take place?
  - → Statistical/mathematical methods? Previous experience?
  - → Actual experiments?
    - » How were they performed? What differed from actual outcome?
    - » What equipment was used?
  - → Facts obtained from third parties?
    - » Often: What is “typical” in business → Ask others what they do/expect others to do/write in contracts/…
    - » Who was asked for information and who actually answered
- What was the result and how likely it is
  - → Is it a law of nature or is this a possible result, which sometimes might perhaps occur?
    - » “Hard” results are desired, but **don’t** state more than justifiable!
  - → Only mention what is important for the questions
    - » No additional research!

Method of evaluation and results

- Answer the questions in detail: „Yes“ or „No“ is inacceptable
  - → Another expert must be able to exactly verify your results and check, whether the facts support the conclusions and whether the methodology used is sound
  - → Try to write in a way so that laymen can understand and follow the reasoning as well
- State clearly if no results could be reached
  - → And what might be done to improve the situation
    - » Expensive experiment, a lot of work, missing data/objects, …
- Describe possible sources of errors
  - → What was not investigated and why
  - → What other methods exist and why they were not used
- Never draw legal conclusions
  - → Remain on the level of technical facts and conclusions

Back matter

- Summary: Brief repetition
  - → Each question should be answered briefly
    - » Only the result, not why this is the outcome (→ see before)
- Signature: Date, signature of expert, stamp
  - → Note: In Austria the stamp is required also for private expertises if performed by an official court expert
- Possible additions:
  - → Glossary: Explanation of terms used in the expertise
  - → Addendums: Screenshots, photos, handbook copies, …
- Not included should be:
  - → General literature: Only literature directly used for facts or conclusions; no “background” material
    - » Neither as copy nor as citation
  - → Full evidence: Returned to owner/court or archived
  - → Copies from the court file

Tips for reading/writing

- First: Check whether questions fall in your area of expertise
  - → You can ask for another expert to complement you or decline
- Keep it short and simple: No scientific explanations or backgrounds for the approach used
  - → But in oral examination you should be able to do this!
- Do not discuss whether one witness is more believable than another → Provide alternative results for both versions
  - → The judge must decide whom to believe!
- You should answer the questions from your own past experience of from experiments
  - → Citing literature is insufficient!
- Keep the costs in mind
  - → Private expertise: Contract
  - → Court expertise: Upper limit (rules for extension etc.)

Tips for reading/writing

- Never ignore/change/minimize the importance of facts, because they do not fit your explanation
  - → No conclusion is better than a wrong one (liability!)
- Keep it short and simple
  - → To be read by non-experts with precious time
- Add “interactive” elements to the pure text
  - → Graphics, photographs, drawings, videos etc.
    - » They are often much better suited than a written description!
    - » Electronic delivery of an expertise should be no problem today
- Do not criticize the law or provide solutions to their problems
  - → You should assess **this** solution, not build **another** one!
    - » Exception: “What can be done to remedy the problem?”
- Never show sympathy or antipathy to any party
  - → This is typical ground for removal
    - » Impartiality must not only exist; it must also look like it

Tips for reading/writing

- An expert has no executive power
  - → If a party refuses access to facts (e.g. computer or data), you can solely inform the judge
    - » Private expertise: No possibility at all against third parties!
  - → The judge may then order the police/… to aid you!
  - → Austria: You may request witnesses to appear and ask them
    - » But if they don't appear, keep silent etc. → See above!
      - – There are no sanctions either!
- Keep exact records of all activities (start & end time, equipment & personnel, activity): Invoice!
- Never contact only one party
  - → Every contact must always involve all parties
    - » Includes letters (→ send registered!), E-Mails (→ CC), …
    - » Investigations at one party: Other party must have possibility to participate (= be present)
  - → If they have an attorney → You must contact him/her!

An expertise in court

- Rules vary in each country → Very general ones here only
- Typical elements of experts in court:
  - → Explanation of their qualification (curriculum vitae)
    - » Previous experience with expertises
    - » Academic titles, “fame” in science/profession
    - » Practical experience in this area
  - → Reading their expertise (almost always omitted)
    - » Often only a brief summary of facts, methodology and results
  - → Questions regarding their methodology and results
    - » Usually based on another private expertise
    - » Justification why not using a different method
    - » Whether another expert may ask questions (directly/indirectly) varies widely (but in some way it is always possible)
- Attention: Lawyers are trained in rhetoric!
  - → Surprise questions, pressure, etc. often occur!

Common attacks on experts/expertises

- “He/she is not qualified”: Works almost never!
  - → Attention: You may work only in your area of expertise; if this is exceeded the attack is almost certain to be successful!
- “Something was ignored”: Some fact/measurement is missing, which would alter the results
- “There exists a different methodology”: Which might be newer, better, more validated, … or not
- “Contradictions exist”: This is typically a serious problem!
  - → If not in the written expertise, then they may try to lure you into some through questions and rhetorics
- „Alternative explanation“: Suppose some other facts, the result would be the same/different
  - → You need to prove that these facts did not (measured)/could not have (conclusions from other measurement) occurred

Exemplary structure: Analysis of some damage

- What has been damaged in which way?
- What was the cause for the damage?
  - → Possible/impossible/probable/real cause
  - → Would damage have occurred if the cause did not happen?
  - → Is cause suitable for the damage in abstract/general way?
- In whose area did the cause occur?
- Has this person ignored an obligation?
  - → Which/what did the person instead/why obliged
  - → What is the objective carelessness?
- Can this person be reproached for this?
  - → Knowingly ignored/required care ignored/could have known the result and that it would occur?
- Would the damage have occurred if this person had fulfilled the obligation and performed carefully?

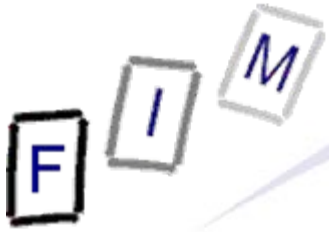
Exemplary structure: Analysis of some damage

- Did the injured also cause the damage?
  - → Can this person be reproached for this and why?
- If yes, which part of the cause is his?
  - → Who could have prevented the damage more easily?
- What is the amount and extent of the damage?
  - → What damage did occur and what will occur in the future?
    - » Certainly, probably, perhaps?
  - → Can the damage be repaired and how much would this cost?
  - → How large is the reduction in value for the damages which cannot be repaired?

Note: This is the full program – Only look into those parts requested by the court/client!

Conclusions

- Be careful when writing an expertise
  - → Important limits: What you may/should do
  - → Private expertises must be impartial as well
- When reading expertises: Read between lines
  - → What was the exact question?
    - » Private expertises: “Steering” the result often through this!
  - → What was not mentioned?
  - → What alternative explanations/methods do exist?
- Assessing an expertise
  - → You should be knowledgeable about the subject area
  - → Any doubtful methods? Conclusions valid for facts?
    - » Alternative explanations?
      - – Through a different area of expertise (e.g. influence of the activity of the sun on computers through solar wind)?



Questions?

Thank you for your attention!