Mag. iur. Dr. techn. Michael Sonntag

Introduction to 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

What is "Computer Forensics"?

- Computer Forensics (CF) is obtaining digital evidence
  - » Analogue evidence is usually not considered here: Use "ordinary" forensics to gather/evaluate
    - – Analogue computers are almost non-existing today!
  - → This may come from running systems or parts of them
    - » Hard disks, flash drives, PDAs, mobile phones, telephones, copiers, “pads” etc.
  - → Can be evidence for computer crimes (computer fraud, hacking, …) or any other crime (documents with plans for x) or for various other uses
- One indispensable issue is "data integrity"

Data is easily changeable:
Evidence is **then and only then** usable in proceedings, if it is **ensured**, that it **has not been changed**!

What is "Computer Forensics"?

- Other definitions:
  - → "Analytical techniques to identify, collect, preserve and examine evidence/information which is magnetically stored or encoded"
    - » Problem: "magnetically" → Flash disks, running systems?
    - » Better: "in computerized systems and their parts"
  - → "We define computer forensics as the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communi-cations, and storage devices in a way that is admissible as evidence in a court of law."
    - » Focus on legal proceedings; there are many other uses as well!
      - – Note that this almost the "highest" form: If evidence is sufficient for criminal proceedings, it can be used for everything else as well!
  - → "A technological, systematic inspection of the computer system and its contents for evidence or supportive evidence of a crime or other computer use that is being inspected."

What is "Computer Forensics"?

- The main elements:
  - → Has something happened at all?
    - » Random effect, bugs, …
  - → When did it happen?
    - » How long had the attacker access to out files?
  - → What has happened and what are the effects?
    - » What are the results from the intrusion/…and what is their direct and indirect "cost"?
  - → Who was responsible for it?
    - » Can we identify an IP address or a person?
  - → How did he do it?
    - » So we can block this in the future
  - → Why were we attacked?
    - » Just “some computer” or deliberate attack; damage/gain; …
- Generally: Uncovering what really occurred

“Evidence”

- Circumstantial evidence (“Indiz”):
  - → A hint, which (alone or together with others) allows to conclude that a certain fact exists
- Evidence (“Beweis”):
  - → A hypothetical situation is accepted as a fact by the judge (rarely: jurors) because he is convinced of it
    - » The circumstantial evidence is presumed to be true
  - → Types of evidence are often strictly regulated
    - » Note: This is a legal distinction and has typically no influence on what can be used as evidence. They are just treated differently.
      - – Example: A witness is treated differently than objects
  - → Used to fulfil the burden of proof
- In English the difference is more vague!

"Burden of proof"

- Note: Not "Obligation to prove"!
  - → You are not required to prove anything … unless you want to "win" the proceedings!
  - → If something cannot be proven, this is disadvantageous for the party which bears the burden of proof
    - » False → Obvious; Practically important: Unknown, no evidence/ witnesses, expert could not find anything conclusive…!
- Typical basic rules:
  - → You state that something is true → You have to prove this
  - → Civil procedures: Everybody proves what would be advantageous for them (and: must claim it; legal problem!)
  - → Criminal procedures → State must prove everything!
  - → If the court is convinced (different levels in law!), the burden of proof switches to the other party to prove the opposite
- Explicit deviations/special rules exist in many laws

Digital evidence

- Digital evidence is
  - → Stored in computers: Disks, memory, …
    - » Not: Printouts, fingerprints on CD-ROMs etc.
  - → Being transmitted between computers: (W)LAN, E-Mails, …
    - » Not: Voice telephone communication (but …!) etc.
- Analogue evidence:
  - → Fingerprints, fibres, body fluids, physically damaged disk, …
- Evidence requires interpretation.
  - → What does it mean that this Bit is “0”?
  - → An E-Mail header exists: Who added it? What does it mean?
  - → Requires a lot of tools: Are they working correctly?
  - → How many steps of interpretation are necessary?
  - → How reliable is the interpretation?
- We will talk only about digital evidence in this course!

Legal considerations

- Computer forensic evidence should be
  - → Admissible: Don't collect anything, which would not be allowed in court
    - » It is useless, and probably illegal too!
  - → Authentic: The evidence should be tied to the incident
    - » Don't go on fishing expeditions
  - → Complete: Not only the "damaging" parts, but all of it
    - » Don't suppress or ignore anything else
      - – If in doubt, collect too much and ignore it later in evaluation!
  - → Reliable: Collection, handling, and evaluation should ensure veracity and authenticity
    - » See "Chain of Custody"!
  - → Believable: Should be believable and understandable in court
    - » And for laymen too (accused, jury, …)
- "The truth, the whole truth, and nothing but the truth"

The basic principles of CF

- No action to secure/collect evidence should affect its integrity
  - → It becomes much less worth/completely worthless!
- Examiners should be trained
  - → Only investigate as far as your knowledge goes
- All activities should be logged
  - → Seizure, examination, storage, and transfer
    - » Complete chain of custody (including its security measures)
  - → Documented, preserved, and available for review
    - » Proof for the chain of custody
- Investigations must be accurate and impartial
  - → Computer forensic ≠ prosecutor/attorney/judge
    - » Describe what was actually found
      - – And what should have been found, but was missing!
    - » Describe how reliable these facts are
    - » Describe what conclusions can reasonably be drawn from it

When to use CF?

- To provide digital evidence of specific activity
  - → In general, proving non-activity might also be the goal, but this is more difficult and only sometimes possible!
- For legal proceedings
  - → Criminal cases: Child pornography, (computer) fraud, ...
  - → Civil cases: Hacking, information theft, industry espionage, …
- Recovering data
  - → (Inadvertently) deleted information
- Identifying weaknesses
  - → After a break in, identify the method employed to prevent it in the future
- Identifying the attack/attacker
  - → Verify, whether an incident actually happened and who was responsible for it

Problematic example of CF

- "Prove, that we did not receive this E-Mail"
- Can we really do that?
  - → We can "easily" prove the receipt of the E-Mail, we just have to find it on the mail server (or traces of it)!
- But proving the negative?
  - → If we don't find any trace on the mail server, this means
    - » we did not search enough,
    - » it was there, but later on accidentally deleted and overwritten,
    - » it was there and then cleverly deleted, or
    - » it was never on the server at all (deleted in transit, …)!
  - → But there is normally no way to prove which of these options describe what actually occurred
- Potential options: Third parties (logs, replies, …), traces of destroying evidence (no proof, but bad in court!)

When to use CF? Concrete examples

- Misuse of ICT by employees
  - → Unauthorized disclosure of data
  - → Internet (WWW, E-Mail, …) abuse
  - → Deleted/damaged information
- Exploiting ICT
  - → Industrial espionage
  - → Hacking of systems
  - → Infiltration (zombie, trojans, viruses, …)
- Damaging ICT
  - → Web page defacements
  - → Denial of Service attacks
  - → Crashing computers

When to use CF?
More (prosaic) examples

- Any normal crime
  - → Plans on computer
  - → Tracing communication or money
- Computer crimes
  - → Phishing, "money mules" etc.
- Disputes between companies
  - → We did deliver the product
  - → The delivery was too late, defective, …
  - → Is the price "appropriate"
- Companies vs. consumers
  - → Details: See above!
  - → Addition: Often "computer company" vs. "laymen"

When NOT to use CF!

- Immediately acting when having any suspicion
  - → Plan first: Evidence is destroyed very easily!
  - → Locate an expert for doing this type of computer forensics
- At the last minute: Do it as soon as possible
- Because I'm interested: Girl/Boyfriend, spouses etc.
  - → Pot. typical area for CF, but should not be used "lightly"!
- "Special" groups are involved
  - → Representatives, medical doctors, attorneys, clergy
    - » These are often privileged regarding evidence
- Because it is against the company policy/immoral/…
  - → If the (suspected) behaviour is not illegal, it is much more difficult to do it legally!
- Use your own staff for important investigations
  - → Use external independent experts (=**third** party!)

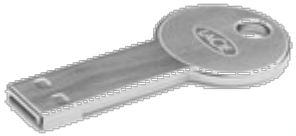
Who should/may use CF?

- Authorization required for accessing data
  - → See privacy laws!
- Live monitoring, hacking, password cracking etc. tools are legally "dangerous"!
  - → Possession alone might be criminal
    - » Good explanation and evidence for its necessity/legal use might be required!
- Personnel to "do" CF:
  - → System administrators in their own area
    - » With restrictions, additional permissions/consent/…!
  - → Experts for courts or private investigations
    - » "Expert" is not a legal/protected name → Anyone can use it!
  - → Everyone on their own system
    - » Note: A second person (e.g. husband/wife) uses the system → Consent by this person is necessary!

Where to find evidence

- Disks: Hard disks, USB-Disks, floppy disks, tapes, …
  - → The typical "storage medium"
  - → Note: These can be very small and very easily hidden
    - » They might also pose as "normal" objects
      - – Example: USB-Stick in pocket knife!
- Devices: Mobile phones, PDAs, MP3 players, USB sticks, game consoles, …
  - → Directly or in disks contained therein
  - → Not a storage medium, but usually may contain arbitrary data
    - » In addition to the "normal" data like music, contacts etc.!
- Recorders: Cameras, audio recorders, GPS trackers, TVs,…
  - → Similar to devices: Own data + any other stored data
- Digital copiers/printers
  - → Might add a serial number to each copied/printed sheet!
  - → May contain old scanned pages

A few examples of hidden USB keys…













Types of evidence

- Who was it: Identifying information
  - → Typical data: IP addresses, login names, passwords
    - » Language of the words used may also be interesting!
- What did he do: Traces of actions
  - → Typical data: Log files, shell history files, event log
  - → Especially important: Various application-internal logs and non-standard configurations
    - » The “standard” files are more likely to be cleaned by attackers!
- What did he add: Data itself
  - → Typical data: Additional program code, user accounts, program configurations
    - » Code: New/changed programs, modified source code
- What did he remove: Remains of data
  - → Typical data: Deleted files (destroyed data as well as his own “intermediate” files), encrypted files

Technical problems of CF

- Anything done to a system changes it
  - → Especially problematic for running systems
  - → Usually less of a problem for hard disks
    - » Reading data might change the content microscopically …
- You can never trust the system under investigation
  - → It may be hacked, modified by the owner etc.
- Proving you did not change anything is difficult
  - → You must be "above suspicion" and take precautions
- The past can never be known
  - → We can only find hints what might have possibly been
    - » The content could have been manufactured by someone!
    - » This can be pretty good evidence, but no absolute proof
- Not everyone knows everything
  - → Every forensic examination is limited by the examiner!

Systematic problems of CF

- Identifying the attacker: IP addresses are typ. the only traces of “hacking”; often they cannot be identified
  - → No information available anymore
  - → Used a proxy (=other hacked computer; commercial proxy service) without any logs on that one
- Finding traces: If the attacker is good, once he has compromised the system he can hide his tracks very well
  - → Note: It is very easy to forget something, but you can hide almost every trace!
    - » Exceptions: Already backed up, external systems (network sniffers/IDS on other system not yet hacked, …)
- Note: Many investigations are successful
  - → E.g. child pornography is difficult to hide and still "use"
  - → The culprit may not even once forget to perform all security precautions (and when he does, he won't immediately notice that he forgot!)

Bias of the investigator

- Very dangerous and must be held back as far as possible
  - → To avoid it completely is probably impossible for a human …
- Dangers:
  - → Limitation of investigation
    - » "This can't be found here", "I'm sure this didn't happen", …
  - → Limitation of interpretation
    - » You find a picture of a naked child: Is it child pornography in the legal sense? Or just a picture of your newborn child?
  - → Limitation of certainty
    - » "Obviously this was the reason"
- Common: Confirming a theory instead of disproving them
  - → Therefore: Explicitly look for things which would invalidate your current assumption
    - » E.g. "File was copied; if so, then MAC should …" → Are they?

An increasing problem of CF: Networking & Security

- Today much data is not stored on "the" computer anymore
  - → Cloud Computing (e.g. Amazon Simple Storage Service; S3)
  - → Webmail accounts, remote harddisks, VPN networks to other systems, FTP server, bulletin boards, "online harddisks"
    - » Example: RapidShare and similar services
- Obtaining a copy of one system is often not enough today!
  - → Find traces of the existence of remote information
  - → Find traces of the remote information itself
    - » Caches, paging file, file slack, local copies, …
  - → Try to access this remote information
    - » By seizure, copying, access over the network, …
- Encrypted disks are difficult
  - → Obtain keys from memory of running system if possible
  - → See also TPM (Trusted Platform Module)

The sequence of actions in CF (1)

- Secure and isolate
  - → Remove all other personnel
  - → Keep reliable witness (police, other third persons)
    - » To protect against "The investigator added this data!"
- Record the scene
  - → Photograph, write down
    - » Example: Mouse on left or right side? → Left-/Right-handed
    - » How are the systems connected (WLAN!)?
    - » What is the current state (running; screen content; …)
  - → In many cases there is quite a mess + lots of computers/devices/…
    - » You won't remember exactly where the disk was and whether it was powered (especially after some month/years)
      - – Example: Disk behind desk? Fell down or deliberately hidden?
      - – Example: Computer running → Might act as a server

The sequence of actions in CF (2)

- Conduct a systematic search for evidence
  - → Especially: Notes with passwords, hints for online services used, storage mediums (USB sticks, flash cards etc.)
    - » More "conventional" search, but important
    - » E.g. steganography impossible without programs → Disks, …
  - → Printouts in waste paper basket, …
  - → Stacks of empty storage media (→"commercial distribution")
- Collect and package evidence
  - → Keep it safe (no loss/destruction) and secure (no changes)
    - » Secure wrapping; external influences
    - » Especially: Magnetic media and magnet fields
      - – Modern harddisks are quite resilient, but not all media are as safe (e.g. magnetic stripe cards)!
    - » Flash cards, USB sticks, etc.: Static electricity
  - → Ideally: Make copies there and package & take both!

The sequence of actions in CF (3)

- Maintain chain of custody
  - → Keep log on who has access and restrict this access
- Inspect and evaluate data
  - → The main aspect we are going to cover here!
  - → Perhaps triage: Immediate brief investigation
    - » What to impound, already some illegal material found → arrest
  - → Detailed investigation in lab (from copy of media!)
  - → Create report:
    - » What was done, what was found, what was not found, what should have been found, how searched, confidence in results, …
- Present the results
  - → In a report
  - → Potentially also before the court
    - » Oral (cross-)examination probable
- Potentially answer questions/respond to counter-expertises

The order of volatility

- Registers, memory caches
- Routing table, arp cache, kernel statistics
- Established network connections, running processes
- Memory
- Temporary file systems (Ramdisks)
- Media in use: Disks in use
- Remote data (on other systems)
- Backup media: Disks not in use, tapes
- WOM: CD-ROMs, DVDs

Evidence should be secured/collected in this order !

- Separately: Analogue material
  - → Physical configuration, paper, fingerprints, DNA, …

Practical sequence

- Document system and real time
- Show active processes
  - → Plus environment, libraries, loaded modules, …
- List current network configuration
  - → Established connection, listening sockets
    - » Plus all data, e.g. which application they belong to
- Copy of memory
  - → Complete or processes only, depending on possibility
    - » Complete copy typically required administrator login!
- Duplicate swap space
  - → Could be deleted/modified during shutdown
- Stop system (see later!)
- Duplicate storage mediums

More in separate lecture!

Chain of Custody

- Guaranteeing **identity** and **integrity** of the evidence
- Requirements:
  - ❶ Making sure the piece of evidence on hand is the same as was taken from the suspect/scene of crime/….
    - » Serial numbers → All harddisks/USB/… look exactly the same!
  - ❷ Making sure there was no tampering with it
    - » Witnesses of actions, trust in the person
  - ❸ Making sure of the transition to the next custodian
    - » Who got it next, i.e. when was a chance for tampering
      - – Lying around somewhere? Handed to an untrusted person? …
  - → Repetition of ❷ and ❸ until the presentation in court
- Note: Digital evidence has a very nice property here: Hash values can reliably prove "no tampering"!
  - → Acquire as early and trustworthy as possible: **"Since then"**!
  - → Store it "securely", e.g. on paper with signature of third person

Chain of Custody

- You have to document
  - → Where, when, by whom was evidence discovered & collected
    - » Plus: “Identity” of the evidence
      - – Example: The harddisk with serial number s was found on desk x by person A at time t
  - → Where, when, by whom was evidence handled or examined
    - » Plus: How it was examined
      - – Example: Person A investigated it at time t with program P in lab L
  - → Who had custody of the evidence during what period
    - » Plus: How was it stored then
      - – Example: Person A stored it in the safe in the lab L at t1
  - → Changes of custody: When and how did the transfer occur
    - – Example: Person A gave it personally to person B at time t
    - – Example: It was sent by registered mail from A to B at time t with package number y

Data hiding methods

- Numerous approaches to hide data exist :
  - → Through the operating system
    - » Mark as "hidden", "system", ...; use ADS; “dot-files”
  - → File extension modification: "order.txt" → "cmd.com"
  - → RAM slack: End of file → End of sector
  - → File slack: End of file → end of cluster
  - → Partition slack: End of partition → end of track
  - → Disk slack: End of last partition → end of disk
  - → Unallocated/bad/reserved sectors
  - → Delete file/partition; format disk
  - → Steganography
  - → Encryption: Not really hidden, but “unusable”
- Attention: Several methods are "unstable", i.e. further actions might destroy the data → Using such methods is complex!
- Many approaches require special programs (hint of existence!)

Computer forensics vs. encryption

- CF does work, but doesn't bring usable results if the data dis-/recovered is encrypted
  - → Depends strongly on the kind of encryption!
- For some programs decryption software is readily available
  - → Especially the integrated encryption of MS Office and Zip!
  - → Sometimes based on weaknesses or short keys
    - » But otherwise just brute force attacks: High computing power, special software, and long time may be necessary!
- If really good encryption is used, there is almost no chance of decryption without the key (or brute force)
  - → One of the reasons for hidden searches: Get at the data before/after it has been en-/decrypted!
  - → But: Very often passwords are known words (→ lists!), are written down somewhere, stored in a safe, …
    - » Important to search the environment for any clues!

What is “Steganography”?

- Steganography: Hiding messages
  - → The intention is that there is no sign that data exists at all
- Typical "recipients": graphics, HTML, text, executables
  - → Common problem: Only a small part of content data can be used for hiding information → Large "cover" for little "content"!
- Areas of use:
  - → Where encryption is illegal
  - → When the fact of communication itself should be hidden
- First encrypt, then employ steganography
  - → Makes detection through statistics much harder!
- Relation to computer forensics:
  - → Hiding data in "inaccessible" places is steganography too
  - → Examples: Various slack spaces, alternate data streams
    - » Rather easy to uncover, if presence is known!

Problems of Steganography

- Not very resilient:
  - → Data hidden in images is easily destroyed through recoding
  - → Text can be reformatted
- Not all base data is suitable:
  - → Many files are exactly "known": E.g. OS files cannot be used to hide data within them
    - » See also the problems caused by signed code!
- Complicated to use: Additional tools necessary
  - → These can be found on the computer, disks, USB sticks, …
    - » But need not necessarily be installed!
- Large pieces of seemingly important base material needed
  - → This is not always available or is a hint to hidden data
- Requires a high level of knowledge to be "good"
  - → Free tools are available, but these are often easily detected!

CF vs. Steganography

- In practice, Steganography seems to be rather rare
  - → There are much easier methods for hidden communication!
    - » E.g. the personal ad columns with certain pre-defined texts
    - » If the text to hide is very long (or multiple pictures, videos), Steganography is problematic even today
- Still, looking for hints that it has been applied should be part of every investigation
  - → Are there any traces of Steganography programs?
  - → Is there suspicious data?
- Brute force attacks, e.g. using steganalysis programs on all images on a computer, are probably less useful
  - → Requires a long time and it is improbable to find anything
    - » Mostly the programs only "support" specific tools for hiding!

De-Duplication

- Data often exists in numerous copies
  - → Installation package and installed version
  - → Temporary files, old versions
  - → Quoted content (E-Mail sequences!)
  - → Full copies in different locations
    - » E-Mail with CC/BCC, local file vs. stored on server (“Windows offline files”)
- De-duplication can reduce the work/duration significantly
- Potential problems:
  - → When is something a duplicate?
    - » Is a quoted mail one? Or is this something different?
  - → Which is the “original” (if we care about this)?
  - → How to exclude the duplicates?
  - → How to keep the references to the duplicates?

Securing evidence: General considerations

- Evidence must be secured in a "trustworthy" way
  - → Nobody should later be able to question the authenticity
- Evidence should be collected as fast as possible, but without destroying anything
  - → This might mean keeping some devices powered, but others without power
    - » Supply with power: Mobile phones, PDAs, tablets, fax, …
    - » Store without power: Flash disks, hard drives, computers
  - → Disconnect any communication to/from the device
    - – Attention: Not necessarily immediately!
    - » E.g. mobile phones: Shielding (no powering off!)
    - » Computers: Network cables, phone lines, serial lines etc.
  - → Check with other forensic experts: Fingerprints
    - » Obtaining traces may damage electronic media!

Securing evidence

- Secure the scene
  - → Preserve potential fingerprints, ensure personnel safety
  - → Immediately restrict access to computers
    - » Physically; electronically comes next!
  - → Document current state (hardware & software)
- Secure the computer as Evidence
  - → If the computer is "OFF", do not turn it "ON"
    - » Disconnect all power sources; unplug from wall AND computer
    - » Place evidence tape over each drive slot
    - » Photograph/diagram and label back of components with existing connections
    - » Label all connectors/cable end to allow reassembly as needed
    - » Package components and transport/store components as "fragile"
    - » Keep away from magnets, radio transmitters, heated seats, etc.
- Interview all persons/witnesses

Securing evidence: Online computers (1)

→ If the computer is "ON"

» Stand-alone computer (non-networked)

– Consult computer specialist

– If specialist is not available

» Photograph screen

» Disconnect all power sources; unplug from wall AND computer

» Continue as with offline computer!

» Networked or business computers / Routers

– Consult a computer specialist for further assistance, because pulling the plug could:

» Severely damage the system

» Disrupt legitimate business

» Create officer and department liability

- Please note: Typical procedure for non-experts

→ Experts will (try to) acquire the runtime-state first!

Securing evidence: Online computers (2)

- Better: Obtain as much information from the running system as possible; only then "shutdown" the system
  - → General rule: Do not alter the state (On → On, Off → Off)!
- ❶ Obtain a copy of the complete state
  - → Copy of the complete memory
    - » With as little changes as possible!
      - – Some additional software MUST be started for transfer!
  - → Output of various "state" commands, e.g. running processes, open network connections, open files/shares, …
- ❷ Remove power cable from computer
    - » Generally some files might be destroyed, so the computer might not boot anymore. But much less data is lost/changed in this way than when shutting it down!
      - – "Delete paging file on shutdown", "Clear privacy data when I close Firefox", …
  - → Not from wall socket: There might be a UPS somewhere!
  - → Laptops: Remove accumulator (both if present) as well

Pulling the plug

- Other recommendations are bit more sophisticated
  - → Servers: Shutdown
    - » Much data can be destroyed when a file/database/E-Mail server is "killed", which can be a problem for companies
      - – Data is lost, computer must be reinstalled/backups restored, …
      - – Could be problematic for investigation too: Garble files, ToC, …
    - » Little danger of deletion/modification scripts
      - – These might be shut down at any point in time by someone else (e.g. by UPS in case of power failure!)
  - → Workstations: Pull plug
    - » Little damage to be done by killing
    - » Usually full control by a single person → Traps much likelier
    - » Restore much quicker and easier
    - » Affects only a single person, not a whole huge company!
  - → Appliances: Pull plug
    - » Typically built to survive this without any damage
    - » The runtime data must be copied before, of course!

The Heisenberg principle - Analogon

- It is impossible to completely capture an entire running system at any point in time
  - → Every kind of "copying the state" will change the state itself!
- The goal to reach:
  - → With as little changes as possible
  - → Without distortion (like installing additional software)
  - → Without bias (like adding hardware/software)
    - » With additional hardware, the data state alone **can** be captured completely and without its modification (→ Theoretically!)
- Decisions are necessary, what to do (and with what tools!)
  - → Generally: Try to obtain as much information as possible without changing too much
  - → Trivial examples: Display running processes and photograph the output on screen
    - » Even better: Use your own (statically linked) program from a CD

Interviewing personnel/witnesses

- Information to obtain:
  - → Owner
  - → User names, passwords
    - » PW: Account, BIOS, E-Mail, configuration, network, ISP, applications, token codes, …
  - → Procedures for access (log in method)
  - → E-Mail addresses, online services/applications used, ISP
  - → Purpose of the system, person(s) using it
  - → Security schemes (self-destruct systems; e.g. delete scripts)
  - → Offsite data: Backups, online replications, …
  - → Documentation of the system: Version numbers
  - → Existence & use: Encryption, Steganography!
- Note also when information is **not** provided!
  - » Or what turns out to be incorrect
  - → Won't help the investigation, but may be important in court

Guiding the search for information

- The aim of the search is most important
  - → Is it a search for "something illegal", a specific crime, or whether the image "xyz.jpg" is present on the computer?
  - → Uncovering all information that is recoverable is possible, but also a lot of work (and therefore extremely expensive!)!
- Assessing the proficiency of the suspect
  - → What "hiding" can reasonably be expected?
    - » If unknown, always assume the worst, i.e. expert techniques!
- When to stop:
  - → If something matching has been found or must all, respectively most of, such data be recovered?
  - → Financial considerations (expenses)

Information according to crimes

- Electronic intrusion
  - → Configuration files
  - → Executable programs and source code/scripts
  - → Open ports, running processes (esp. servers)
  - → Logs: Activity, connection, programs, communication, …
- Fraud
  - → Address books, calendars: Physical, E-Mail etc.
  - → Images: Cheques, currency, Western Union, signatures, products, …
  - → Credit card data, esp. CVC
  - → Office documents: Letters, spreadsheets, databases
  - → Banking/accounting software: Dedicated and online
  - → Internet activity: Logs, caches, cookies, …
  - → Account information: eBay, banks, …
  - → Communication history: E-Mails, chat logs

Information according to crimes

- Undesirable communication (threats, spam, mobbing)
  - → Address information: E-Mail, telephone, …
  - → Documents: Background information, diaries, legal etc.
  - → Communication: Letters, E-Mails, SMS, chat logs, …
  - → Internet activity: Cache, logs, cookies
  - → Accounts: Online communication facilities
  - → Images: Person, products, fakes
  - → Software: Mass mailers, text/image/PDF generators
  - → Financial information: Accounts, banking

Information according to crimes

- Violence: Child abuse/pornography, domestic v., death
  - → Images, especially hidden ones, and videos
  - → Date and time stamps
  - → Internet activity: Cache, logs, cookies, access time, searches
  - → Software: Communication, photo, P2P
  - → Address information and communication: E-Mails, chats, tel.
  - → Documents: Legal, medical

Information according to crimes

- Identity theft
  - → Personal information: Name, address, credit card, …
  - → Communication: Especially copies of other person's, obtaining/buying information online
  - → Software: Generators (names, credit card numbers), imaging (scanner, photo modification)
  - → Images: Certificates, forms, signatures
  - → Documents: Forms, letters, orders, …
  - → Electronic signatures
  - → Internet activity: Cache, logs, searches

Information according to crimes

- Copyright
  - → Software: P2P, CD/DVD-burning, encryption, recoding, key generators, cracks
  - → Documents: Serial numbers, authorization information
  - → Internet activity: Cache, logs, searches, cookies
  - → Images: Covers, license forms
  - → Communication information: E-Mail, chat
  - → Accounts: Web-Sites, FTP, shops
  - → Date and time stamps

Admissibility of evidence (1)

- Digital information is no evidence as such alone
  - → Illegal image on disk? How did it come to be there? Unknown!
    - » Was it the accused, someone else through his account, the police, a hacker who broke in over the network, … ?
    - » Additional information can help if present
      - – Physical access to computer, logon-history, encryption etc.
- One very important aspect is the person collecting and interpreting the evidence
  - → If this person is trusted → no modifications took place later
  - → When a conclusion is stated as a fact, the person will not be very useful, as judges will not believe them
    - » Fact = Observable
      - – Example: Free space on disk is 100 MB
    - » Conclusion = Fact + interpretation/general rules
      - – Example: Windows will be slow (no swap file) and programs might crash if more space is required for log files/backups/…

Admissibility of evidence (2)

- Continental law:
  - → Generally all evidence is admissible, regardless how obtained
    - » Exclusions exist, but are few/very rarely apply!
    - » But what evidence is worth depends on
      - – How it was collected and stored
      - – By whom it was collected
      - – Who analyzed it
      - – How it was analyzed
      - – Whether the conclusions are supported by facts
      - – Whether the conclusions are "state of the art"
  - → Typically the judge (or rarely a jury) decides
- Common law:
  - → Facts might also be fixed by parties!
    - » If agreed upon, judge/jury cannot discuss it any more
  - → Esp. USA: "fruit of the poisonous tree" doctrine
    - » Evidence obtained unlawfully may not be used

Admissibility of evidence (3)

- Note: There is no "court-approved forensic SW"!
  - → Neither in the USA nor the EU/Austria there is a certification/approval for what "things"/"devices"/"SW" might/must be used for investigation
- But: Investigation must be done according to state of the art!
  - → Employing the "usual" SW is typically state of the art
  - → Other software might also be used, but could require additional explanation in court
    - » Typically the case in the USA!
  - → Europe: Person of investigator is often more important
    - » Officially certified court expert, reputation, experience etc.
    - » Method is only important if another expert criticizes it
      - – Or the court knows/suspects from other cases that it might be suspect/wrong/incorrectly applied, …

Documenting actions

- All actions during an investigation must be documented
  - → This starts with acquiring the evidence!
    - » Writing down and photographing when/how the computer was found, which state it was in, etc.
- Running systems: Every single command entered must be documented with the time and the complete results
  - → Ideally the log and the result should be stored as a file with a checksum to verify its integrity
- Offline systems:
  - → The state must be exactly documented, e.g. checksums over the whole disk
  - → Every step of the examination should be documented like in a running system
- Generally: Document also tools (make, version, …) used!

Documenting actions

- Methods of documentation
  - → Pen & paper: For non-electronic actions
    - » Disk is duplicated, computer is unplugged, …
  - → Other “analogue” documentation: Photos, audio commentary
    - » Might be digital today, but are not the action itself
  - → Electronic log: If possible, e.g. protocol of all commands issued during investigation
    - » Depends on the system/software used
- Chain of custody: Important for the documentation too!
  - → Pen & Paper: Number pages, don’t leave partly empty, sign every page, separate signature for “end of document"
  - → Digital documentation: Photos, audio logs, … should contain metadata (e.g. time and serial number of camera) if possible

Documenting actions: “script”

- The “script” command (*nix) copies the in- and output to a file
  - → Note: The commands should be only “normal” text commands
    - » E.g. “vi” will not be represented correctly!
  - → End with Ctrl+D (or “exit”)
- Example: “script –f log.txt”
  - →
```
Script started on Tue 05 Jul 2011 01:24:13 PM CEST
[root@mail backup]# date
Tue Jul  5 13:24:18 CEST 2011
 [root@mail backup]# ls –al
total 36
drwxr-xr-x  3 root root  4096 Jul  5 13:24 .
drwxr-xr-x 25 root root 12288 May 17 21:49 ..
drwxr-xr-x  5 root root  4096 Jul  5 04:06 db
-rw-r--r--  1 root root     0 Jul  5 13:24 log.txt
[root@mail backup]# exit
exit
Script done on Tue 05 Jul 2011 01:24:32 PM CEST
```
- Don’t forget: Hash value, read-only, store on other disk, …!

Documenting the time/time difference

- Very important for the evaluation later
  - → Note: We can't know the difference between the computer time and the real time at some point in the past: Only now!
- The time on the investigation system should be very precise
  - → Use NTP or similar for synchronisation (and take care of timezone and DST!)
- Time on the investigated system should NOT be changed!
  - → Only the difference should be documented
- Practical problem: How to do this!
  - → Solution 1: Document time on investigated system and manually add (paper, not file!) the "real" time at that moment
  - → Solution 2: Connect both systems, redirect output to second system, call "date" on first system, note timestamp of created logfile (not the timestamp within it!) on second system

Common errors of computer forensics (1)

- No incident response plan
  - → At some time an incident will happen. If there are no plans what to do in which sequence, most probably the wrong things will be done.
  - → Requirements:
    - » Who should be alarmed when
    - » Rules for escalation
    - » Guidelines for quickly assessing the problem
      - – Without changing anything!
    - » Should be clearly documented and available without the system
      - – I.e., ideally on paper!
- Underestimation of the incident
  - → Third parties or other systems might also be affected
    - » Example: Laptop was stolen → Data on laptop is “gone”
      But: Remote access to company servers possible?

Common errors of computer forensics (2)

- Delayed detection of an incident or response to it
  - → E.g. the earlier the disks are copied, the more information will still be present
  - → Reduction of the time the attacker has for performing changes or hiding his tracks
    - » As soon as it is definite that an incident occurred → "full alarm"!
    - » Keep any "preliminary" investigations for later & for experts
- Management is informed late or incompletely
  - → External investigations might be costly: The management needs full information (as far as available)
  - → Responsible for business continuity/contingency measures outside of the IT area
  - → Decision on whether to involve the police or through whom
  - → Special measures might be necessary → Must be authorized

Common errors of computer forensics (3)

- Incomplete documentation of activities
  - → Chain of Custody (see above)
  - → But also for other (non-IT) measures
    - » Might be extremely important in the legal area: Did you do everything (or: enough) to reduce the damage (insurance!)
    - » Did you do enough to prevent damage to third parties (liability!)?
  - → If documentation exists, going to court might still be an option later (although with less valuable evidence)
- Digital evidence is protected inadequately
  - → If the option for a court proceeding should remain open, very strict standards for access to data are necessary
    - » Checksums for everything!
  - → Evidence should be stored on read-only devices (today's hard disk sizes typ. prevent this!), offline, and physically secured

Final report: General information

- Identity of the examiner
- Identification of the case, e.g. case numbers
  - → Who commissioned the report?
- Subject of examination
  - → List of and serial numbers of disks/components/…
  - → Source of the equipment
    - » Personally taken from suspect, received from police/court etc.
- Procedural history
  - → When was what piece of evidence received, examined, passed on, reported upon, …
    - » Chain of custody!
  - → Description of examination: Who did what when in which way
    - » Which techniques were used; state of the art?

Final report: General information

- Results and conclusions
  - → Facts (see next slide): What was found
  - → Conclusions: What can be derived from that?
    - » This must conform to a very high degree and state assumptions!
      - – Example: Time of computer matches "real" time, file access date is 12.12.06 (facts) → File was accessed at that time
        - » Note: Changing the clock, who used the computer, network connections, …?
    - » Includes a reliability assessment:
      - – Not necessarily with a percentage, but should have it if possible!
      - – "Might perhaps be", e.g. 10%
      - – "Almost assuredly", e.g. 99,999%
  - → What was not investigated?
    - » But might be interesting
    - » Reason for this "omission"
    - » What therefore cannot be deduced from the things investigated
    - » What could be in there and what could never (?) be in there

Final report: Content

- Summary of findings (non-technical language!)
- Detailed findings:
  - → Specific files matching the search
    - » And other files supporting the findings
  - → String searches, keywords searches, and text string searches
  - → Internet-evidence: Web traffic analysis, chat logs, cache files, E-Mail, newsgroup activity, ICQ/Skype/… activity
  - → Graphic image analysis
  - → Ownership status of all files found
    - » Who of the users owned them/when were they created/accessed
  - → Techniques used to hide data or limit access to it
    - » Steganography, encryption, hidden attributes/partitions/streams
    - » Incorrect file names (e.g. JPEG files with ".bin" extension)
- Annex: Printouts, digital copies, documentation

Confidence levels

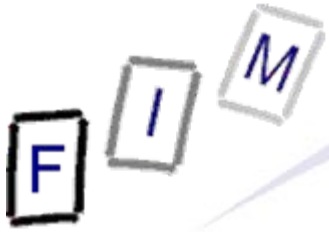
- Any conclusions should contain a reliability assessment
  - → There is always some uncertainty…
  - → But: Didn't we want to find out the truth, the whole truth and nothing but the truth?
    - » Yes, but the world is imperfect (and money often limited ☺!)
- Informal categories:
  - → Possibly (Eventuell)
  - → Perhaps/Very possibly (Vielleicht)
  - → Probably (Wahrscheinlich)
  - → Most probably (Sehr wahrscheinlich)
  - → Almost definitely (Mit an Sicherheit grenzender Wahrscheinlichkeit)
  - → Definitely (Mit Sicherheit): This category is absent!

Confidence levels: Casey's C-Scale

Certainty level	Description/Indicators	Qualification
C0	Evidence contradicts "known" facts.	Erroneous/Incorrect
C1	Evidence is highly questionable.	Highly uncertain
C2	Only one source of evidence that is not protected against tampering.	Somewhat uncertain
C3	The source(s) of evidence are more difficult to tamper with but there is not enough evidence to support a firm conclusion or there are unexplained inconsistencies in the available evidence.	Possible
C4	Evidence is protected against tampering or multiple independent sources of evidence agree (which are not protected against tampering).	Probable
C5	Agreement of evidence from multiple independent sources that are protected against tampering. However, small uncertainties exist (e.g. temporal error, data loss).	Almost certain
C6	The evidence is tamper-proof and unquestionable. No other explanation is possible at all.	Certain

Conclusions

- Obtaining some information from hard disks is easy
  - → Ensuring it is complete **and** usable in courts is difficult!
  - → There is only a **single chance** …
- A wide variety of hardware exists, which must be treated differently and contains various information
  - → Specialization is needed for in-depth investigation
- The huge amount of data on modern computers is a problem
  - → Try to reduce the scope of investigation
    - » Lists of "known good" files
  - → Automate examination
    - » Keyword searches, deleted file recreation etc.
- Expensive software needed
  - → Some investigation also possible with cheaper tools
  - → Open source software available partly



Questions?

Thank you for your attention!

Literature

- Casey, Eoghan: Digital Evidence and Computer Crime[2], London 2004
- NIJ Report: Forensic Examination of Digital Evidence: A Guide for Law Enforcement. http://www.ojp.usdoj/nij
- NIJ Report: Electronic Crime Scene Investigation: A Guide for First Responders. http://www.ojp.usdoj/nij
- dns: An introduction to: Computer Forensics http://www.dns.co.uk/NR/rdonlyres/5ED1542B-6AB5-4CCE-838D-D5F3A4494F46/0/ComputerForensics.pdf
- RFC 3227: Guidelines for Evidence Collection and Archiving