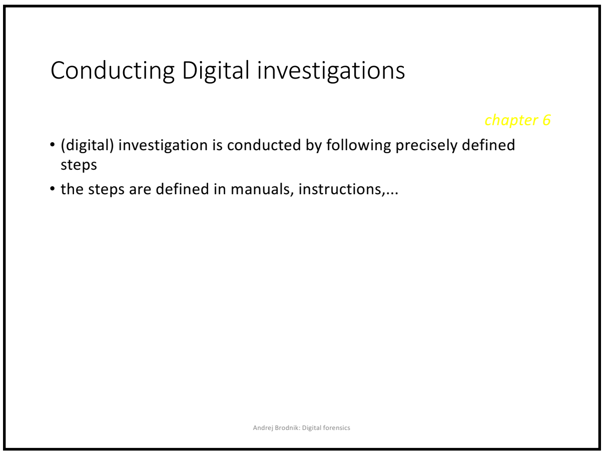
Digital forensics

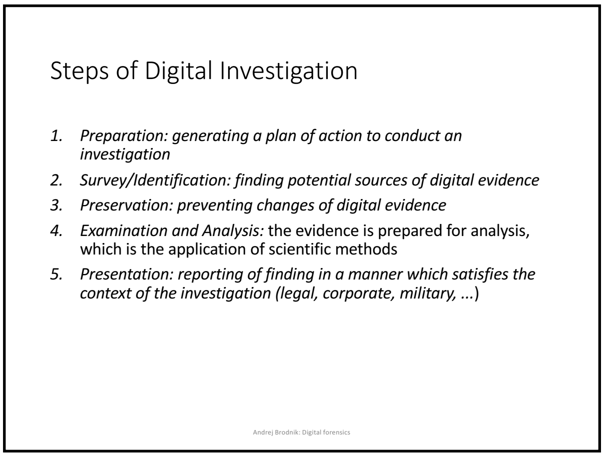
Andrej Brodnik



Conducting Digital investigations

chapter 6

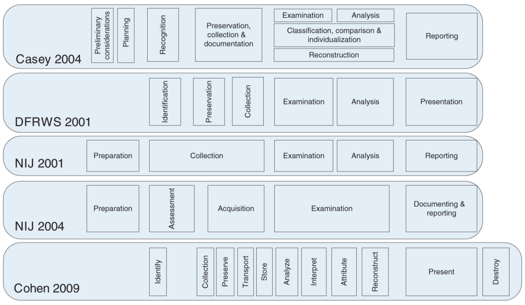
- (digital) investigation is conducted by following precisely defined steps
- the steps are defined in manuals, instructions,...



Steps of Digital Investigation

1. *Preparation: generating a plan of action to conduct an investigation*
2. *Survey/Identification: finding potential sources of digital evidence*
3. *Preservation: preventing changes of digital evidence*
4. *Examination and Analysis:* the evidence is prepared for analysis, which is the application of scientific methods
5. *Presentation: reporting of finding in a manner which satisfies the context of the investigation (legal, corporate, military, ...*)

Steps of Digital Investigation



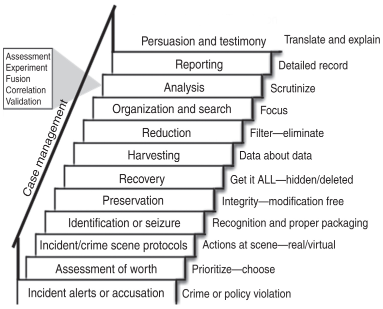
Digital Investigation Process Models – Physical Model

- model with the more established investigative process (Carrier, 2003)

	Phase Goals (Physical)	Phase Goals (Digital)
Crime scene preservation	Securing entrances and exits and preventing physical changes to evidence	
Crime scene survey	Walking through scene, identifying obvious and fragile physical evidence	
Crime scene documentation	Photographs, sketches, maps of evidence, and crime scene	
Crime scene search and collection	In-depth search for physical evidence	
Crime scene reconstruction	Developing theories based on analysis results and testing against evidence	

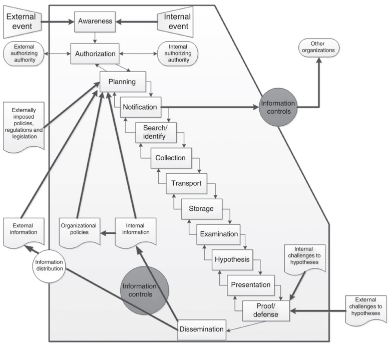
Digital Investigation Process Models – Staircase Model

- Casey & Palmer, 2004
- digital investigators, forensic examiners and attorneys work together
- not a linear progression of events but it may be necessary to take certain steps more than once



Digital Investigation Process Models – Evidence Flow Model

- Ó Ciardhuáin, 2004
- goes beyond the steps required to preserve and examine digital evidence
- completely describes the flow of information in a digital investigation



Digital Investigation Process Models – Subphase Model

- Beebe & Clark, 2005
- a multilayered framework, taking the steps common in other models and adding subphases with defined objectives to help investigators implement each step properly
- main phases are:
  1. preparation
  2. incident response
  3. data collection
  4. data analysis
  5. findings presentation
  6. incident closure

Digital Investigation Process Models – Subphase Model

- example: objectives for file system analysis
  1. reduce the amount of data to analyze
  2. assess the skill level of suspect(s)
  3. recover deleted files
  4. find relevant hidden data
  5. determine chronology of file activity
  6. recover relevant ASCII data
  7. recover relevant non-ASCII data
  8. ascertain Internet (non-e-mail) activity history
  9. recover relevant e-mail and attachments
  10. recover relevant „personal organizer“ data (calendar, address books, ...)
  11. recover printed documents
  12. identify relevant software applications and configurations
  13. find evidence of unauthorized system modification (malware)
  14. reconstruct network-based events

Digital Investigation Process Models – Roles and Responsibilities Model

- Ieong, 2006
- FORZA – providing the framework of roles and responsibilities in digital investigation

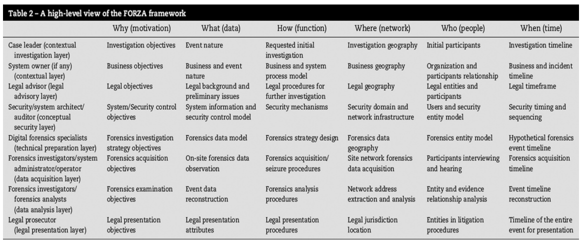


Table 2 – A high-level view of the FORZA framework

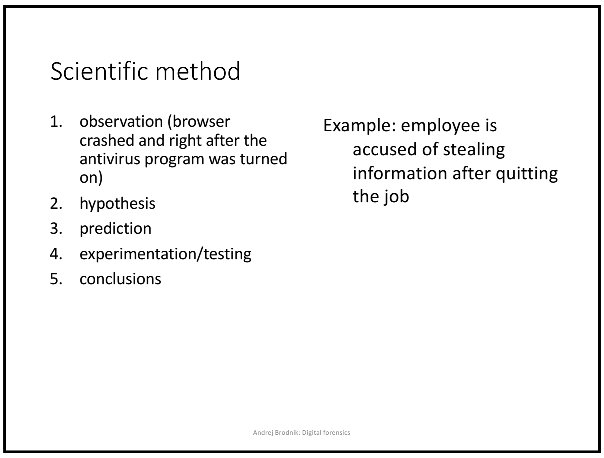
	Why (motivation)	What (data)	How (function)	Where (network)	Who (people)	When (time)
Case leader (contextual investigation layer)	Investigation objectives	Event nature	Requested initial investigation	Investigation geography	Initial participants	Investigation timeline
System owner (if any) (contextual layer)	Business objectives	Business and event nature	Business and system process model	Business geography	Organization and participants relationship	Business and incident timeline
Legal advisor (legal advisory layer)	Legal objectives	Legal background and preliminary issues	Legal procedures for further investigation	Legal geography	Legal entities and participants	Legal timeframe
Security/system architect/ auditor (conceptual security layer)	System/Security control objectives	System information and security control model	Security mechanisms	Security domain and network infrastructure	Users and security entity model	Security timing and sequencing
Digital forensics specialists (technical preparation layer)	Forensics investigation strategy objectives	Forensics data model	Forensics strategy design	Forensics data geography	Forensics entity model	Hypothetical forensics event timeline
Forensics investigators/system administrator/operator (data acquisition layer)	Forensics acquisition objectives	On-site forensics data observation	Forensics acquisition/ seizure procedures	Site network forensics data acquisition	Participants interviewing and hearing	Forensics acquisition timeline
Forensics investigators/ forensics analysts (data analysis layer)	Forensics examination objectives	Event data reconstruction	Forensics analysis procedures	Network address extraction and analysis	Entity and evidence relationship analysis	Event timeline reconstruction
Legal prosecutor (legal presentation layer)	Legal presentation objectives	Legal presentation attributes	Legal presentation procedures	Legal jurisdiction location	Entities in litigation procedures	Timeline of the entire event for presentation

Data Acquisition

- starting point of every investigation is the accusation or incident alert
- authorization of investigation
  - written authorization from attorneys
  - search warrant
- threshold considerations – decision is made, whether or not the investigation will continue
- transportation – chain of custody
- verification of gathered evidence
- case management – binds together all of the activities and outcomes

Applying the Scientific Method in Digital Investigations

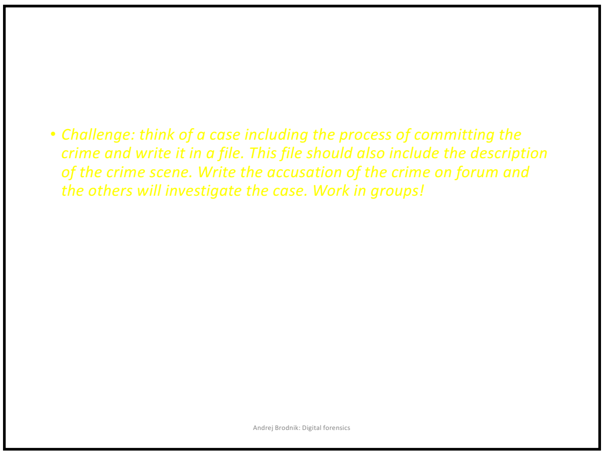
- investigation must be based on scientific methods
  - formation and evaluation of Hypotheses
- steps:
  - preparation
  - survey
  - preservation
  - examination
  - analysis
  - reporting and testimony



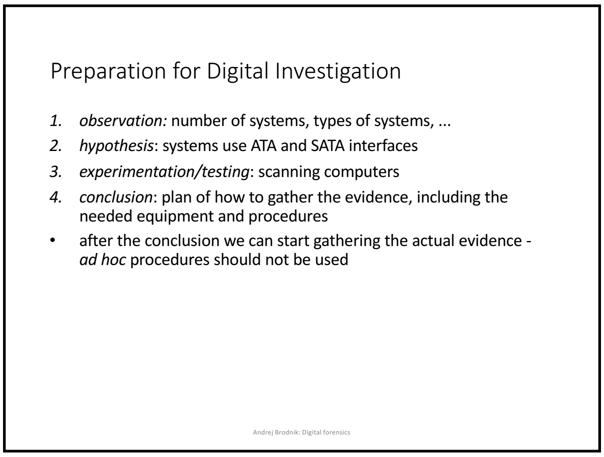
Scientific method

1. observation (browser crashed and right after the antivirus program was turned on)
2. hypothesis
3. prediction
4. experimentation/testing
5. conclusions

Example: employee is accused of stealing information after quitting the job



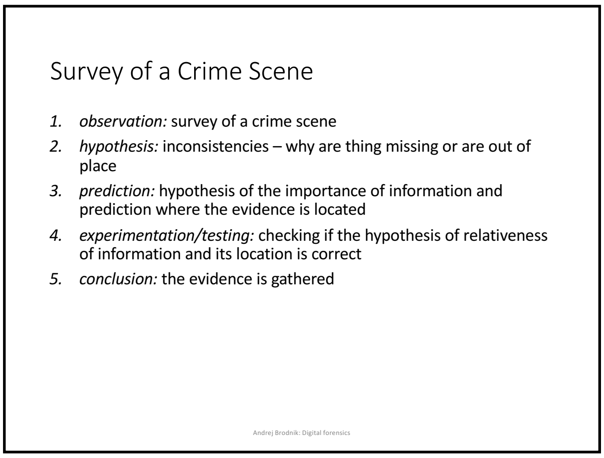
- *Challenge: think of a case including the process of committing the crime and write it in a file. This file should also include the description of the crime scene. Write the accusation of the crime on forum and the others will investigate the case. Work in groups!*



Preparation for Digital Investigation

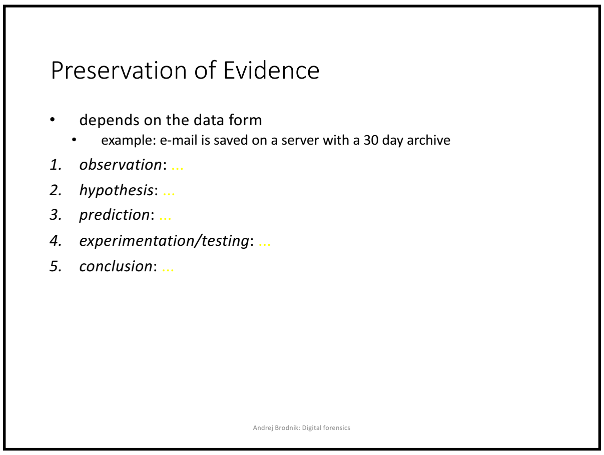
1. *observation:* number of systems, types of systems, …
2. *hypothesis*: systems use ATA and SATA interfaces
3. *experimentation/testing*: scanning computers
4. *conclusion*: plan of how to gather the evidence, including the needed equipment and procedures

- after the conclusion we can start gathering the actual evidence - *ad hoc* procedures should not be used



Survey of a Crime Scene

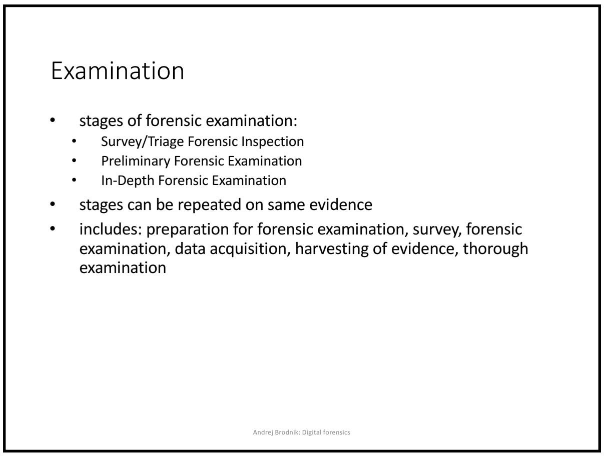
1. *observation:* survey of a crime scene
2. *hypothesis:* inconsistencies – why are thing missing or are out of place
3. *prediction:* hypothesis of the importance of information and prediction where the evidence is located
4. *experimentation/testing:* checking if the hypothesis of relativeness of information and its location is correct
5. *conclusion:* the evidence is gathered



Preservation of Evidence

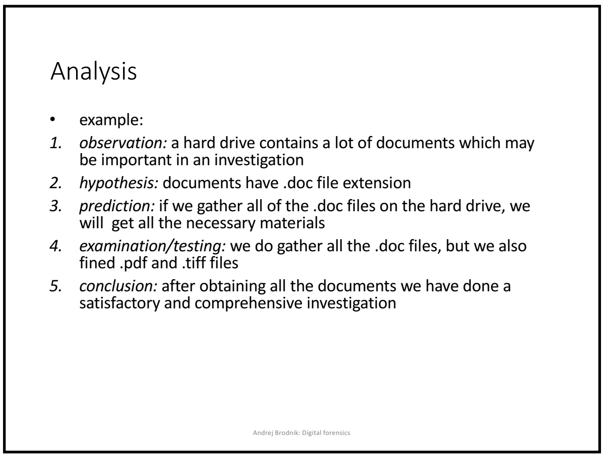
- depends on the data form
  - example: e-mail is saved on a server with a 30 day archive

1. *observation*: …
2. *hypothesis*: …
3. *prediction*: …
4. *experimentation/testing*: …
5. *conclusion*: …



Examination

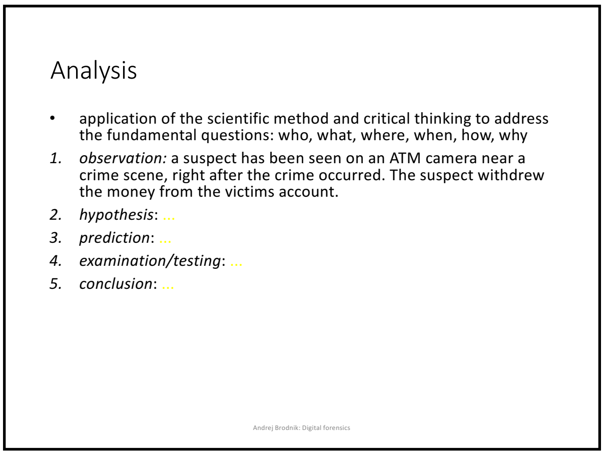
- stages of forensic examination:
  - Survey/Triage Forensic Inspection
  - Preliminary Forensic Examination
  - In-Depth Forensic Examination
- stages can be repeated on same evidence
- includes: preparation for forensic examination, survey, forensic examination, data acquisition, harvesting of evidence, thorough examination



Analysis

- example:

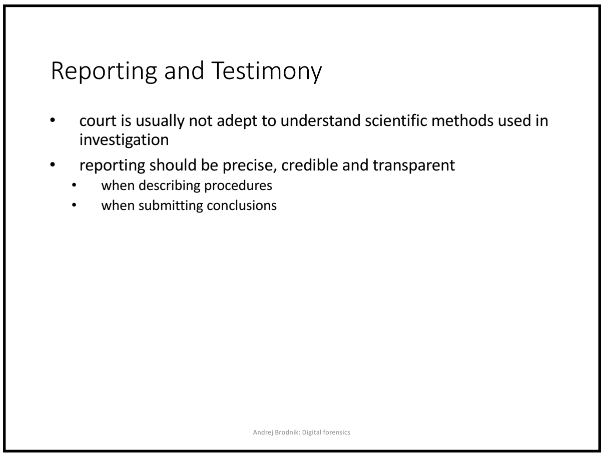
1. *observation:* a hard drive contains a lot of documents which may be important in an investigation
2. *hypothesis:* documents have .doc file extension
3. *prediction:* if we gather all of the .doc files on the hard drive, we will get all the necessary materials
4. *examination/testing:* we do gather all the .doc files, but we also fined .pdf and .tiff files
5. *conclusion:* after obtaining all the documents we have done a satisfactory and comprehensive investigation



Analysis

- application of the scientific method and critical thinking to address the fundamental questions: who, what, where, when, how, why

1. *observation:* a suspect has been seen on an ATM camera near a crime scene, right after the crime occurred. The suspect withdrew the money from the victims account.
2. *hypothesis*: ...
3. *prediction*: ...
4. *examination/testing*: ...
5. *conclusion*: ...



Reporting and Testimony

- court is usually not adept to understand scientific methods used in investigation
- reporting should be precise, credible and transparent
  - when describing procedures
  - when submitting conclusions

- *Challenge:* read the case example from the book and study the investigation.

  In this case, Jill observes unusually high numbers of failed logon attempts to a server that contains plans and details of Corporation X's newest product, code named FastJet . She contacts the system administrator for the system and, after a quick review of recent system logs, he confirms that there has been unauthorized use of the administrator account on the system. There is a strong indication that a security breach has occurred.

  Comment on the forum.

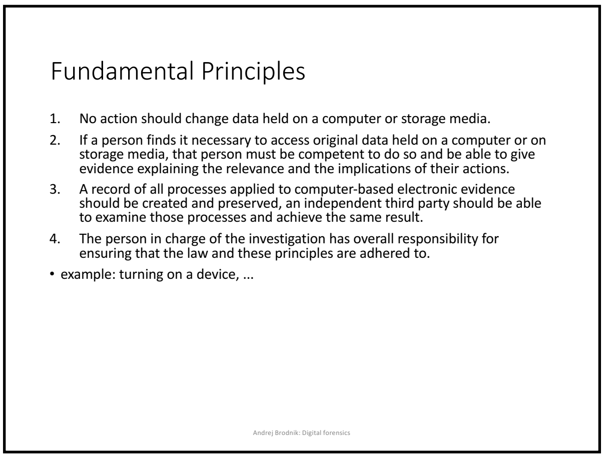
Handling a Digital Crime Scene

- evidence is digital, the crime scene is strictly physical
- There are a number of published guidelines that present fundamental principles of handling a crime scene

Handling a Digital Crime Scene

chapter 7

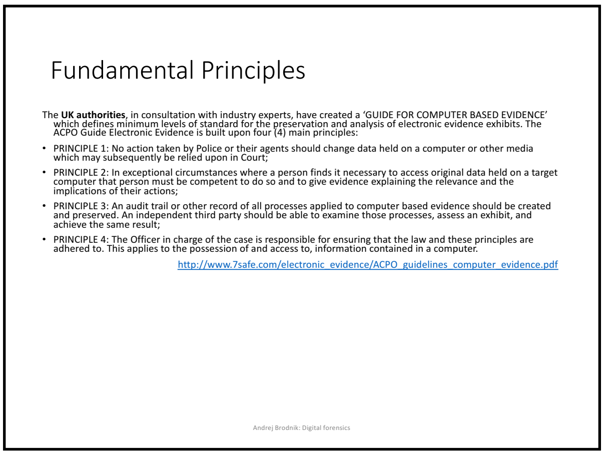
- one of the most practical guideline documents:
  - *The Good Practice Guide for Computer Based Evidence*, (*ACPO guide, Association of Chief Police Officers*)
  - http://www.afentis.com/forensic-science-articles/acpo-guide-electronic-evidence
  - http://7safe.com/electronic_evidence/index.html#



Fundamental Principles

1. No action should change data held on a computer or storage media.
2. If a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
3. A record of all processes applied to computer-based electronic evidence should be created and preserved, an independent third party should be able to examine those processes and achieve the same result.
4. The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

- example: turning on a device, ...

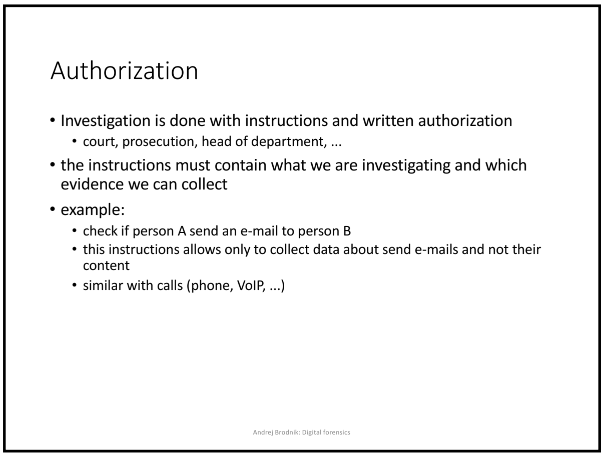


Fundamental Principles

The **UK authorities**, in consultation with industry experts, have created a ‘GUIDE FOR COMPUTER BASED EVIDENCE’ which defines minimum levels of standard for the preservation and analysis of electronic evidence exhibits. The ACPO Guide Electronic Evidence is built upon four (4) main principles:

- PRINCIPLE 1: No action taken by Police or their agents should change data held on a computer or other media which may subsequently be relied upon in Court;
- PRINCIPLE 2: In exceptional circumstances where a person finds it necessary to access original data held on a target computer that person must be competent to do so and to give evidence explaining the relevance and the implications of their actions;
- PRINCIPLE 3: An audit trail or other record of all processes applied to computer based evidence should be created and preserved. An independent third party should be able to examine those processes, assess an exhibit, and achieve the same result;
- PRINCIPLE 4: The Officer in charge of the case is responsible for ensuring that the law and these principles are adhered to. This applies to the possession of and access to, information contained in a computer.

http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf



Authorization

- Investigation is done with instructions and written authorization
  - court, prosecution, head of department, ...
- the instructions must contain what we are investigating and which evidence we can collect
- example:
  - check if person A send an e-mail to person B
  - this instructions allows only to collect data about send e-mails and not their content
  - similar with calls (phone, VoIP, ...)

Authorization

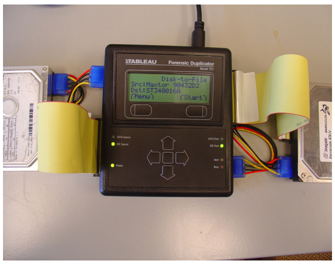
- court must/should ensure that the investigation is not going to violate privacy laws
- The suspect is innocent until proven guilty
  - and even then his privacy must be respected

Preparing to handle digital crime scenes

- preparing a strategy (game plan) before investigating a crime scene
- a plan is very important for protecting the credibility of evidence

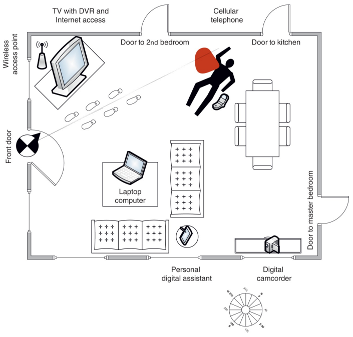
Preparing to handle digital crime scenes – ACPO Guide

- consider the offender's technical skill level
- bringing specific materials, tools and equipment to help preserve and document digital evidence
- consideration of data vulnerability: wireless and network devices, working devices (computers),...



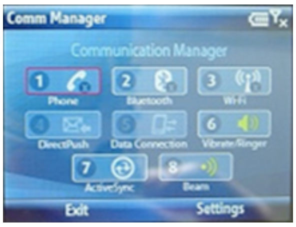
Surveying the Digital Crime Scene

- digital evidence can be found in different places - important to be methodical
- O/I units, manuals for hardware and software, …



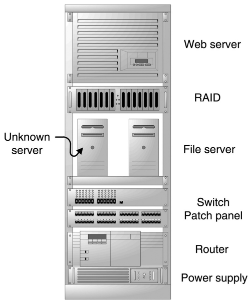
Surveying the Digital Crime Scene

- shut down the device
- record of device shut down



Surveying the Digital Crime Scene

- precise inventory of all devices and their characteristics
- password for access and encryption
- recording findings in accordance with the plan

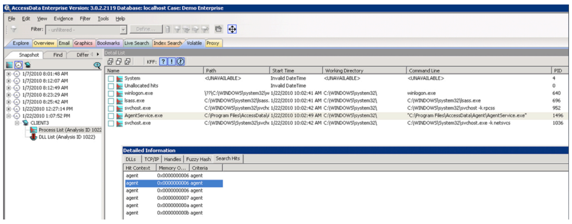


Preserving the Digital Crime Scene

- controlling entry points:
  - video surveillance equipment: disable to protect from outside invasion and saving the information recorded
  - (wireless) networks: disable to prevent remote access
- freezing the networked crime scene
  - copy all evidence, make inventory list and save the evidence
  - securing remote data
  - securing non-digital evidence (fingerprints and biological evidence)

Preserving the Digital Crime Scene

- preparing a plan for preservation of evidence
- remote preservation



Name	Path	Start Time	Working Directory	Command Line	PID
□ System	<UNAVAILABLE>	Invalid DateTime	<UNAVAILABLE>	<UNAVAILABLE>	4
□ Unallocated hits		Invalid DateTime			0
□ winlogon.exe	\??\C:\WINDOWS\system32\w	1/22/2010 10:02:41 AM	C:\WINDOWS\system32\	winlogon.exe	640
□ lsass.exe	C:\WINDOWS\system32\lsass.	1/22/2010 10:02:41 AM	C:\WINDOWS\system32\	C:\WINDOWS\system32\lsass.exe	696
□ svchost.exe	C:\WINDOWS\system32\svch	1/22/2010 10:02:42 AM	C:\WINDOWS\system32\	C:\WINDOWS\system32\svchost -k rpcss	952
□ AgentService.exe	C:\Program Files\AccessData\	1/22/2010 10:02:49 AM	C:\WINDOWS\system32\	"C:\Program Files\AccessData\Agent\AgentService.exe"	1496
□ svchost.exe	C:\WINDOWS\System32\svch	1/22/2010 10:02:42 AM	C:\WINDOWS\system32\	C:\WINDOWS\System32\svchost.exe -k netsvcs	1036

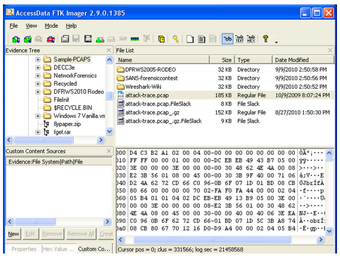
Hit Context	Memory O...	Criteria
agent	0x0000000006	agent
agent	0x0000000006	agent
agent	0x0000000006	agent
agent	0x0000000007	agent
agent	0x000000000a	agent
agent	0x000000000b	agent

Preserving the Digital Crime Scene

- What about currently running devices?
- preserving information on RAM is hard
- but:
  - currently running processes give information about the intrusion into the system
  - encrypted file system is connected and the password is entered
  - unlocked access to remote locations or services
  - …

Preserving the Digital Crime Scene

- on currently running we use conventional forensics tools (FTK)
- second principle of ACPO!!



Sample-PCAPS
DECC3e
NetworkForensics
Recycled
DFRWS2010 Rodeo
FileInit
$RECYCLE.BIN
Windows 7 Vanilla.vm
flypaper.zip
fget.rar

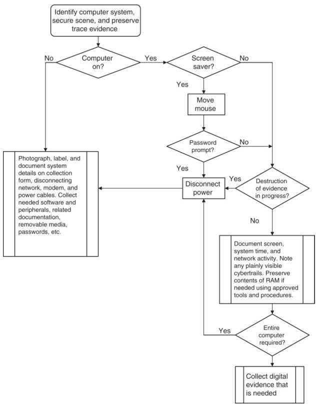
Name	Size	Type	Date Modified
DFRWS2005-RODEO	32 KB	Directory	9/9/2010 2:50:58 PM
SANS-forensiccontest	32 KB	Directory	9/9/2010 2:50:56 PM
Wireshark-Wiki	32 KB	Directory	9/9/2010 2:50:52 PM
attack-trace.pcap	185 KB	Regular File	10/9/2009 8:07:24 PM
attack-trace.pcap.FileSlack	8 KB	File Slack	
attack-trace.pcap_.gz	152 KB	Regular File	8/27/2010 1:50:30 PM
attack-trace.pcap_.gz.FileSlack	9 KB	File Slack	

```
000 D4 C3 B2 A1 02 00 04 00-00 00 00 00 00 00 00 00 ÔÃ²¡···
010 FF FF 00 00 01 00 00 00-DC EB EB 49 43 B7 05 00 ÿÿ·····
020 3E 00 00 00 3E 00 00 00-00 30 48 62 4E 4A 00 08 >···>··
030 E2 3B 56 01 08 00 45 00-00 30 3B 9F 40 00 71 06 â;V···E
040 D2 4A 62 72 CD 66 C0 96-0B 6F 07 1D 01 BD 08 CB ÒJbrÍfÀ
050 80 66 00 00 00 00 70 02-FA F0 FA 44 00 00 02 04 ·f····p
060 05 B4 01 01 04 02 DC EB-EB 49 13 B9 05 00 3E 00 ·´····Ü
070 00 00 3E 00 00 00 00 08-E2 3B 56 01 00 30 48 62 ··>····
080 4E 4A 08 00 45 00 00 30-00 00 40 00 40 06 3E EA NJ··E··
090 C0 96 0B 6F 62 72 CD 66-01 BD 07 1D 5C 3B A8 74 À··obrÍ
0a0 08 CB 80 67 70 12 16 D0-D9 A4 00 00 02 04 05 B4 ·Ë·gp··
```

Cursor pos = 0; clus = 331566; log sec = 21458568

Preserving the Digital Crime Scene

- shut down the system
- disconnect power – where?
  - on PC case – why?
- removing the casing and viewing the interior
  - missing parts, …
- disconnect power to the disks
- in all interventions be aware of the position of the situation :
  - shutting down a computer can cause an explosion ☹
- **consider the offender's technical skill level**☺


Identify computer system, secure scene, and preserve trace evidence
Computer on?
No
Yes
Screen saver?
No
Yes
Move mouse
Password prompt?
No
Yes
Photograph, label, and document system details on collection form, disconnecting network, modem, and power cables. Collect needed software and peripherals, related documentation, removable media, passwords, etc.
Disconnect power
Yes
Destruction of evidence in progress?
No
Document screen, system time, and network activity. Note any plainly visible cybertrails. Preserve contents of RAM if needed using approved tools and procedures.
Yes
Entire computer required?
Collect digital evidence that is needed

- *Challenge: Let's say there has been a crime in the lecture room, in the lobby, in a computer room, … Make a plan for securing the digital crime scene.*

- *Challenge: Work with a colleague. The crime has taken place on his property. The evidence is a picture of the criminal Cefizl that your colleague hides somewhere. Make a plan for preservation of the crime scene and conduct an investigation. Afterwards replace the roles.*