

# Digital forensics

Digital forensics combines computing, law and investigation. This is also a generally interesting subject, involving a range of technical know-how and raising political, legal and ethical questions for discussion.

## How to use

This booklet is a mixture of theory, activities and reference material, so it can be selectively read. The content aims to include both beginner and intermediate levels. It attempts to give an overview and explain essential technical terms; unfamiliar terms can generally be disregarded or looked up as required.

Activities are suggested, for discussions, practical exercises or demos. Technical activities have a Linux (or Mac) and “command line” focus but Windows and GUI (Graphical User Interface) programs are included. Note that some programs and technical points may become dated, but the basic tools and techniques are well established.

This booklet is indebted to the Open University’s M812 Digital Forensics module ( <http://www.open.ac.uk/postgraduate/modules/m812> ), as well as to workshop participants and others.

The author is not an expert in digital forensics or legal matters. This should not be taken as legal advice. It is work in progress; comments / corrections welcome.

**Warning:** Possessing and/or reading this booklet could be used as evidence of knowledge of digital forensics.

<http://www.thebrentc.net/articles/digitalforensics>

[brentc@riseup.net](mailto:brentc@riseup.net)

2017

Version 1.1

<b>Digital forensics</b>	<b>1</b>
Important notes	2
Scenarios and Issues	3
Forensics basics	4
Digital forensics	5
Digital forensic process	6
Digital forensics and the law	7
The UK Computer Misuse Act 1990	8
“Hacking” etc.	9
Various laws	10
“Crime scene” strategy	12
Kit	13
Some computing basics	14
Evidence acquisition	22
Forensic imaging	23
Linux, Mac, BSD [draft]	28
Netcat	29
Low-level data analysis	30
Undeleting	31
Digital forensic artefacts	32
Live forensics [dev]	35
Anti-forensics	36
Forensic readiness	39
Fixes for Kali Linux	40
Windows 3.11	41
Workshop plan	42
Overview	44
Links / further reading	44

## Important notes

- Ensure your computers are backed up; practical forensics carries a risk of damage and data loss.
- Authorisation is required to access any computer, legally and ethically. This likely means working only with your personal computers or systems. Avoid workplace or organisation computer systems.
- Be very cautious with others’ systems even if permission is given; digital forensics can be revealing with potentially unfortunate fallout.

**Discussion: Ethics**

Digital forensics features investigations of computers. Have a think about the ethics around doing digital forensics. You can refer to [Scenarios and Issues](#) below.

## Scenarios and Issues

1. System administrators can find dodgy or illegal material on the systems that they administer..
2. Computing equipment confiscated by authorities and later returned naturally raises questions of whether the equipment is compromised.
3. Shared or “family” computers can complicate forensics and raise privacy questions.
4. Forensic techniques may be used to do data recovery for friends etc.

## Links

SAGE (2003) *System Administrators' Code of Ethics* [Online]. Available at <https://www.usenix.org/system-administrators-code-ethics>

Janet CSIRT (n.d.) *Suggested Charter for System Administrators* [Online]. Available at <https://community.jisc.ac.uk/library/janet-services-documentation/suggested-charter-system-administrators>

## Forensics basics

Digital forensics is based on traditional forensics. This uses scientific method to gather evidence for analysis and ultimately presentation to court standards.

This scientific investigation aims to be reproducible, and a key principle in forensics is the “continuity of evidence” (or “chain of custody”)- being able to prove the history of evidence from acquisition to presentation, required for admissibility.

Pure science is a continuing search for universal truths, but forensics has the practical application to resolve a legal matter- for the UK, “beyond a reasonable doubt” in criminal law and “on a balance of probabilities” in civil law.

The use of evidence in forensics is based on “Locard’s Exchange Principle” that describes the transfer of evidence:

“Wherever he [sic] steps, whatever he touches, whatever he leaves – even unconsciously – will serve as silent evidence against him...”

This is also characteristic of digital evidence, with some uniquenesses.

## Digital forensics

The forensic ideal of evidence continuity is expressed in the ACPO (2012) digital forensic principles:

### **Principle 1**

No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.

### **Principle 2**

In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able 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 digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

### **Principle 4**

The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

In practice, this means taking contemporaneous notes, and using digital imaging. In imaging, an exact copy is carefully taken of the suspected digital evidence. Investigation then works from digital copies, avoiding interfering with the original evidence material.

Digital evidence is unique: exact copies can be made of digital material, and digital evidence can be analysed without causing damage to it. This is generally not possible with physical evidence.

## **Reference**

Association of Chief Police Officers (ACPO) (2012) *Good Practice Guide for Digital Evidence, 5th version* [Online]. Available at

[http://www.digital-detective.net/digital-forensics-documents/ACPO\\_Good\\_Practice\\_Guide\\_for\\_Digital\\_Evidence\\_v5.pdf](http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf)

## Digital forensic process

Digital forensic activities will be part of a larger investigation. Key steps are:

Forensic readiness	A u t h o r i s a t i o n	D o c u m e n t a t i o n
Initialisation of investigation		
Acquisition of evidence		
Analysis		
Reporting		
Closure		

Note the ongoing activities such as obtaining authorisation and maintaining documentation (i.e. “contemporaneous notes”).

### The “police notebook” technique

Using a pre-numbered, tamper-evident notebook, each entry includes date and time, space at the end of a line is filled with a horizontal line, any unused space on a page is also crossed through, and entries are signed. Corrections are made by simple crossing-out and making a new entry; no information is removed.

### References:

*BSI (2016) BS EN ISO/IEC 27043:2016: Incident investigation principles and processes*, London, British Standards Institution.

*BSI (2016) BS EN ISO/IEC 27037: Information technology. Security techniques. Guidelines for identification, collection, acquisition and preservation of digital evidence*, London, British Standards Institution.

Open University (2017) *M812 - Digital Forensics* [Online]. Available at <http://www.open.ac.uk/postgraduate/modules/m812>

Wikipedia (2016) *Police notebook* [Online], 11 December 2016. Available at [https://en.wikipedia.org/wiki/Police\\_notebook](https://en.wikipedia.org/wiki/Police_notebook)

## Digital forensics and the law

- Digital forensics is used for both prosecution and defence.
- Law systems are divided into “criminal” and “civil” strands. Digital forensics are applied in civil investigations as often as criminal cases.
- While there are computer-specific laws and crimes, often computers are simply used to commit conventional crimes, for example fraud. This is increasingly organised crime.
- In modern practice, there are extensive “pre-trial procedures” or “pre-action protocols”, aiming for “efficient” and “fair” trials without surprises. There is a “disclosure regime”; the prosecution reveal their case fully, and the defence must reveal their defence plan.
- Digital forensic investigators may be “expert witnesses” in court. In America, expert witnesses can be “advocational” i.e. work more directly for one side, in the UK there is an overriding “duty to the court”.
- An investigation must satisfy the criteria of being necessary and proportionate as well as authorised. Failure to respect this is likely to result in evidence being inadmissible and possible legal action against investigators. An improper investigation can be challenged on the basis of the UK *Human Rights Act 1988*; rights to liberty, security, fair trial and privacy.

## The UK Computer Misuse Act 1990

The Computer Misuse Act (CMA) was implemented partly in response to the case *R v Gold & Schifreen* (1988). A “shoulder-surfed” admin password for BT systems was exploited, including to get into Prince Philip’s email. Attempts to convict under *Forgery and Counterfeiting Act 1981* failed on appeal. This contributed to calls for specific laws to deal with so-called “hacking” cases, leading to the CMA, with later modifications. Intent is generally sufficient for a crime to be committed. The Act is controversial, for example Section 3A risks criminalising many general-use computer tools.

Computer Misuse Act 1990 1990 CHAPTER 18
An Act to make provision for securing computer material against unauthorised access or modification; and for connected purposes.
Be it enacted by the Queen’s most Excellent Majesty, by and with the advice and consent of the Lords Spiritual and Temporal, and Commons, in this present Parliament assembled, and by the authority of the same, as follows:—
Computer misuse offences
1 Unauthorised access to computer material. ...
2 Unauthorised access with intent to commit or facilitate commission of further offences. ...
3 Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc. ...
3ZA Unauthorised acts causing, or creating risk of, serious damage ...
3A Making, supplying or obtaining articles for use in offence under section 1, 3 or 3ZA ...

### References / further reading:

Great Britain. [Computer Misuse Act: Elizabeth II. Chapter 18](http://www.legislation.gov.uk/ukpga/1990/18/contents) (1990). London, The Stationery Office [Online]. Available at <http://www.legislation.gov.uk/ukpga/1990/18/contents>

Turner, M. J. L. (2016) *Computer Misuse Act 1990 cases* [Online]. Available at <http://www.computerevidence.co.uk/Cases/CMA.htm>



## “Hacking” etc.

There are debates and uncertainties around terms such as “hacking”.

The traditional meaning of “**hacking**” is something like a person who is clever with technology. Malicious and illegal activities are often better described as “**cracking**” (Perrin, 2009), or perhaps simply as “crime”.

Hacking however has a tendency to the “illicit” (Jordan, 2009); in part because it is a creative and challenging working with technology.

“**Hactivism**” is the use of technology for social change, possibly involving illegal activities. Beyond basic “clicktivism”, this can include from activist tech support to “electronic civil disobedience” acts (Vlavo, 2015; Jordan, 2009).

### Discussion: Hacking debate

How do these ideas fit in with law, for example the *Computer Misuse Act 1990*?

## References

Jordan, T. (2009) ‘Hacking and power: Social and technological determinism in the digital age’, *First Monday*, vol. 14, no. 7 [Online]. DOI: [10.5210/fm.v14i7.2417](https://doi.org/10.5210/fm.v14i7.2417) (Accessed 10 May 2017).

Perrin, C. (2009) *Hacker vs. cracker* [Online]. Available at <http://www.techrepublic.com/blog/it-security/hacker-vs-cracker/> (Accessed 10 May 2017).

Vlavo, F. (2015) ‘Framing digital activism: The spectre of cyberterrorism’, *First Monday*, vol. 20, no. 10 [Online]. DOI: [10.5210/fm.v20i10.6139](https://doi.org/10.5210/fm.v20i10.6139) (Accessed 10 May 2017).

## Various laws

These and other laws are relevant in digital forensics. This discusses UK law; other jurisdictions have comparable laws. Law changes so it is necessary to keep up to date. The UK law system is “common law”, meaning that law is built from “case law”, i.e. referring to previous judgements, as well as from Acts of Parliament, etc.

The *Computer Misuse Act 1990* criminalises attempting unauthorised computer access and related activities (see [The UK Computer Misuse Act 1990](#)).

*Fraud Act 2006*: “False representation” with “intent to prejudice [i.e. gain]”. There is also the *Forgery and Counterfeiting Act 1981*, covering “false instruments” for dodgy purposes.

*Privacy and electronic communications regulations 2003*: Anti-spam law, requiring consent and the sender being identified.

Child pornography is banned by the *Protection of Children Act 1978*, a definitional age of 18 set by the *Sexual Offences Act 2003*, and “strict liability” possession by the *Criminal Justice Act 1988*. Extreme pornography is now defined under the *Criminal Justice and Immigration Act 2008*, superseding the *Obscene Publications Act 1959*; “publication of articles to deprave and corrupt” as being too vague for an increasingly tolerant society.

*Prevention from Harassment Act 1997*: Addresses stalking, including cyber, and provides for restraining orders.

*Telecommunications Act 1984 / Communications Act 2003*: Outlaw offensive, obscene, menacing and similar communications, and improper use of public communications networks.

*Theft Act 1968*, Section 21 deals with blackmail (“unwarranted demands with menace”), applicable to RansomWare attacks.

*Regulation of Investigatory Powers Act 2000*: Allows for interception of communications. “Communication” or “meta” can be obtained under warrant and is court admissible. “Interception” or “content” is inadmissible. The Lawful Business Regulations provide exemptions for businesses monitoring their own communications networks.

*Copyright, design and patents act 1988*: Provides exclusive rights for copyright etc. holders, with licence granting. See also *Trade Marks Act 1994*.

*Data protection act 1998*: Provides requirements on processors of personal data and limited protections for data subjects, with some criminal provisions e.g. the “unlawful” obtaining, use, etc. of personal data.

The *Human Rights Act 1998* implements an EU directive. Article 5 affirms the right to liberty and security, Article 6 to fair trial and Article 8 to privacy.

The *Defamation Act 2013* covers slander and libel (“false statement harming reputation”), unless there is a defence, such as it’s true.

*Digital Economy Act 2017*: Stronger criminal penalties for copyright infringements and moves to website age-verifications and website blocking.

*Investigatory Powers Act 2016*: Formalises mass surveillance, interception and sharing of communications, security forces’ “targeted equipment interference” (cracking), and retention of “internet connection records”.

-X-

Civil law features contracts (“legally binding agreement”) and “torts” (civil wrong, including negligence and duty of care failures). If there is good reason, a court can approve a Civil Search Order, an equivalent of a police search with an “independent”, supervising solicitor.

-X-

Investigations are covered by such laws as the *Police and Criminal Evidence Act 1984*, *Criminal Procedures and Investigations Act 1996* and the *Civil Procedure Act 1997*.

-X-

Multiple laws, both criminal and civil, may be applied. For example, industrial espionage or data theft may criminally violate the *Computer Misuse Act 1990* or others, but may be pursued as breach of contract if an employee or business partner is involved.

- X -

Under *Defamation Act 1996*, ISPs and service providers only become liable for defamation if they fail to act following complaints. *Defamation Act 2013* sets out regulations and procedures for website operators to deal with defamation complaints. This is published as the *Defamation (Operators of Websites) Regulations 2013*.

## “Crime scene” strategy

A “first responder” at an incident may need to “secure the scene” and preserve evidence. Some possible activities:

- Obtain necessary authorisations.
- Assess health and safety issues.
- Deal with suspects.
- Control electronic interference (for example others’ mobile phones may interact with networks at the scene).
- Establish a perimeter, with single entry/exit.
- Set up a command station.
- Nominate an evidence custodian.
- Perform preliminary survey, using the “least travelled path”.
- Document the scene using notes, photographs and sketches with measurements.
- Do a full scene search (using spiral, strip, zone, grid or wheel patterns).
- Collect evidence and arrange chain of custody.
- Perform a final scene survey.

Digital forensics may include preserving physical evidence, such as fingerprints etc.

### **Faraday shield your phone**

Part of “crime scene preservation” is preserving evidence; it may be required to keep a mobile device on but prevent network communications.

For proof-of-concept, and fun: Wrap (or aesthetically sculpt) your phone in aluminium foil. This should block all incoming and outgoing signals (try phone in from a different phone).

Notes: Any cable plugged into the phone that extends outside the shield can function as an antenna. When phones are shielded, they can use extra battery power in attempts to reach networks. This shielding also works for “touch” cards, badges etc.

Faraday shielding techniques may be applied in [Anti-forensics](#).

## Kit

(For practice: A laptop is sufficient. Optional useful items are small, clean USB flash drives / memory sticks, live Linux media and other tools such as PortableApps. Access to Windows as well as Linux and Mac systems is helpful).

Notebook and pen (and/or digital equivalent)  
 Lots of storage i.e. external USB drives or flash drives (“memory sticks”).

A forensic workstation/laptop.  
 Live boot forensic Linux distributions on DVD/USB e.g. Kali ( [www.kali.org](http://www.kali.org) ).  
 Windows live and/or “PortableApps” tools  
 Write blocker (hardware or software).  
 Documentation, “cheat sheets”, etc.

Watch.  
 Camera.  
 Tools e.g. screwdrivers, torch.  
 A powered USB hub may be useful (for extra ports and power for USB drives/devices).  
 External CD/DVD drive (for live booting).  
 Anti-static wristband.  
 Faraday shield/material.

Gloves etc.  
 Evidence packaging and labelling materials.

The forensic computer workstation and setup needs to be managed. Consider: tool “validation”, malware protection, evidence storage, information security and privacy.

Tamper-evident bag procedures: To re-open, open at *opposite* end from seal, complete reason for opening, process the evidence, then re-seal the evidence and the old bag in a new evidence bag.

See:

Home Office (2015) [Tamper evident bags](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/488537/Tamper_evident_bags_version_3.0EXT_clean.pdf) [Online]. Available at [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/488537/Tamper\\_evident\\_bags\\_version\\_3.0EXT\\_clean.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/488537/Tamper_evident_bags_version_3.0EXT_clean.pdf)

## Some computing basics

These practical details may be generally useful; for example data recovery can use similar skills.

**Command line and GUI:** While the standard Graphical User Interface (GUI) tools are used, it is often necessary to use the text-based “command line” or “terminal” in digital forensics.

### Using the command line.

1. Find and open the terminal or command line on your computer.
2. The file system is arranged as files within folders. Use combinations of the following commands to explore your file system:

	Linux or Mac	Windows
Show files in current directory	ls	dir
Change directory up	cd ..	cd ..
Change down into <directory> [replace <directory> with the required subdirectory name]	cd <directory>	cd <directory>
Change to “root” directory level	cd /	cd \
Show current directory	pwd	chdir
View <file> content (for text files)	cat <file>	type <file>
Get help	<command> --help (or man <command>) For example: ls --help	<command> /? For example: dir /?

Press up/down arrows for command history, Tab to try autocomplete, and in Linux use Shift-Ctrl-C and Shift-Ctrl-V for copy/paste. When you’re finished, type ‘Exit’ (or press Ctrl-D to exit in a Linux terminal).

You can compare the command line view to the graphical view of files/folders using your operating system’s file explorer program.

In the rest of the booklet, lines with ‘\$’ indicate Linux terminal commands being entered.

**Note:** Commands in this booklet may require the “root” (administrator) user level. To switch to the root level in Linux, enter: su, or: sudo su, or precede commands with: sudo ...

## Command line cheat sheet

Digital forensics is cross-platform. For example while forensic Linux tools are often used, investigating a Windows system requires knowledge of Windows and possibly using Windows-based tools. In this table, DOS refers to the Windows command line. MacOS has a Unix base, like Linux, so many of the same commands, as does the “BSD” family of OS’s.

DOS	Unix	
assign	ln -s	create symbolic link
attrib	chmod	change file permissions
chdir	pwd	display current directory
chdisk	du	disk usage
cls	clear	clear screen
comp /fc	diff	compare files
copy	cp	
date/time	date	show date or time
del/erase	rm	delete file
dir	ls	directory listing
doskey /h	history	get recent commands
find	grep	find matching lines
format	mke2fs	format a disk
help	man	get help
ipconfig	ifconfig	check network configuration
mem	free/top	check memory usage
mkdir/md	mkdir	create directory
netstat	netstat	network info
pkzip	zip	compress a file with ZIP
print	lpr	print file
reboot	shutdown -r now	reboot system
rename/move	mv	rename file or move file
route print	route -n	check routing configuration
tasklist	ps	list of running programs
tracert	traceroute	trace route
type	cat	print file content
ver	uname -a	OS version

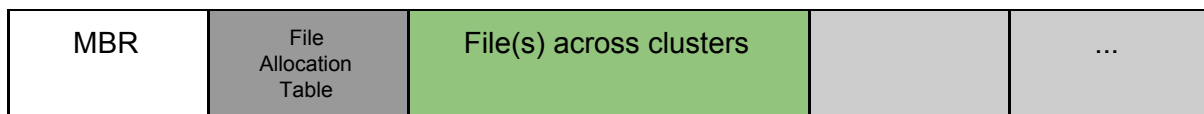
From: SANS (2008) *Windows to Unix cheatsheet* [Online]. Available at:  
[https://digital-forensics.sans.org/media/windows\\_to\\_unix\\_cheatsheet.pdf](https://digital-forensics.sans.org/media/windows_to_unix_cheatsheet.pdf)

## Disk structures [draft]

There are various computer storage medias and setups. Some knowledge of this is necessary to digital forensics; to be able to basically identify what's on a computer, to find data that can be hidden in various ways on computer disks, and to understand file undeleting. A consideration of a traditional hard drive introduces some common features:

- Hard drives are divided into one or more “partitions”.
- A small Master Boot Record area (MBR) of 512MB at the beginning of the drive stores various configuration info.
- A partition will be “formatted” as one of various “filesystem” types.
- Filesystem types have typical uses, for example FAT32 often for USB drives, NTFS usually for Windows, EXT versions for Linux and HFS with Mac.
- Hard drives are divided up into units; “clusters” of “sectors”.
- Files (data, operating system files or programs) are then stored on the formatted partitions, allocated clusters/sectors according to how the specific filesystem operates.
- The common FAT32 arrangement is to have a File Allocation Table (also called FAT), that is an index to the files stored across the filesystem partition [?].
- For technical reasons, files can be fragmented, i.e. not stored in successive clusters (handled using pointers to the address of the next piece).

```
|-----Drive-----|
|-----Partition(s) divided into "clusters"-----|
```



*Figure: Very simplified representation of a drive with FAT formatted partition.*

### Some digital forensic considerations:

- When a file is deleted on filesystems such as FAT32, the space is really only marked as available in the File Allocation Table (by changing the first letter of the filename).
- This means that a file can often be easily undeleted by simply restoring the File Allocation Table record.
- It also means that “deleted” file data is still there until the space is re-used. Even if there isn't an index in the File Allocation Table, data or pieces of data can be found by a low-level perusal of the hard drive, and other techniques such as “file carving”; where clever tools find and extract known file types.  
(See [Low-level data analysis](#) and [Undeleting](#)).



## Checking disk structures

To see which drives are present, from Linux, look in the special /dev folder for all entries starting with 'sd' (sometimes 'hd'):

```
$ ls /dev/sd*
```

On my system, this shows:

```
/dev/sda /dev/sda1 /dev/sda2 /dev/sda3
```

This indicates one hard drive divided into three partitions.

To see information about the filesystems on these, the Linux fdisk command can be used (as root). **Warning:** The fdisk utility can also be used to change drive setups, risking data loss, take care if using these functions.

```
$ fdisk -l /dev/sda
```

This shows:

Device	Boot	Start	End	Blocks	Id	System
/dev/sda1		2048	142577663	71287808	83	Linux
/dev/sda2		144336896	234440703	45051904	b	W95 FAT32
/dev/sda3		142577664	144336895	879616	82	Linux swap

This indicates a Linux formatted partition, with its usual accompanying “swap” space (used for memory caching), as well as a FAT32 formatted partition.

Hard drive partitions need to be “**mounted**” before they can be used, often done automatically by operating systems. Windows allocates drive letters (e.g. C:) to these, and Linux uses file/folder ‘shortcuts’ e.g. /mnt or /media/...

To complete the picture, use ‘mount’ or ‘df’ [diskfree] to see what’s in use:

```
$ df -H
```

This shows:

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/sda1	72G	34G	35G	49%	/
...					
/dev/sda2	47G	17k	47G	1%	/media/user/EE47-DD3D

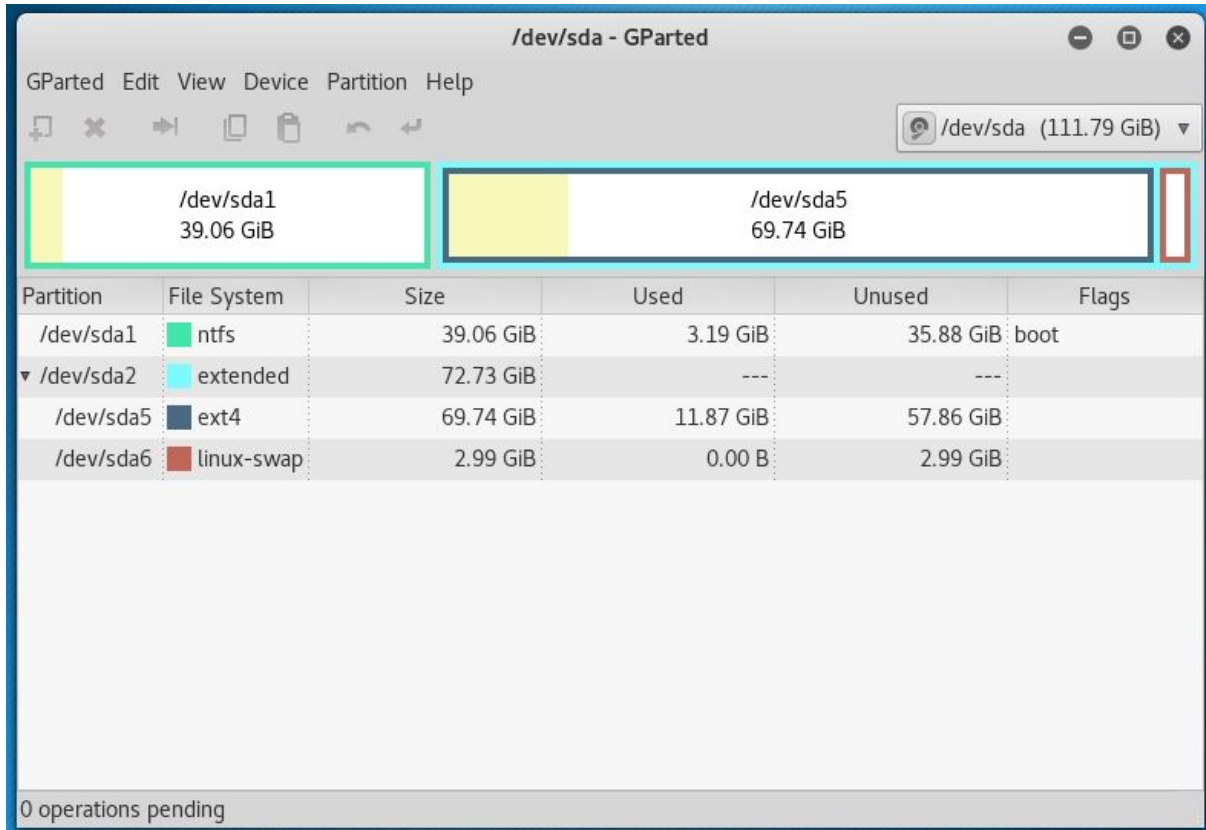
This indicates that the Linux partition is mounted and in use as the main operating system partition, and the FAT32 partition has been mounted with a link in the usual /media directory.

Exit out of root mode for safety:

```
$ exit # or press ctrl-d
```

For Windows, try DISKPART in its command line. Linux often provides gparted as a GUI “frontend” tool.

## Example 2: Disk structure



A typical “dual boot” system- a Windows (ntfs) partition, with a Linux (ext4) partition and it’s “swap space”. Usually only 4 “primary” partitions are possible on a disk, so the “extended” partition setup as above is used to allow more than 4 partitions if required.

This reflects in the /dev directory:

```
$ ls /dev/sda*
/dev/sda  /dev/sda1  /dev/sda2  /dev/sda5  /dev/sda6
```

## Live booting

Usually an operating system (such as Windows, Linux or MacOS) is installed to and runs from a computer hard disk. It is possible, particularly with Linux, to “live boot” a computer from a CD, DVD or USB flash drive with an operating system on it. The operating system then runs in memory only, but can also access the host computer.

This is used in digital forensics, for example to obtain access to a suspect computer without actually using the installed operating system (which would contaminate the evidence). Booting a computer from a live media provides a ‘backside’ view of the computer being investigated- you’re accessing the system without running it. Live booting can be used to obtain a “forensic image” of suspect computer hard drives (see below).

To boot from live media, you will typically need to insert the media, start the computer, and promptly select an option to boot from live media at the computer’s startup (or “BIOS”) point.

### Live booting

1. Find or prepare a live boot medium, typically:
  - a. Download an ‘iso’ file of a Linux distribution.
  - b. Write this to DVD or USB memory stick. This needs to be done in a specific format: look for ‘write an image’ options in burner programs for DVD, try dd or unetbootin on Linux, or Fedora Media Writer on Windows for USB flash drives.
2. Insert the media, switch on the computer, catch the option to choose boot media in the BIOS startup, and select the appropriate media source.

The BIOS boot options vary by computer; try Esc or F12 or look it up for the computer model. You may need to try use any available option(s) to pause computer startup to have time to insert DVDs, etc., or use Ctrl-Alt-Del to reboot for further attempts.

Your mileage may vary with your computer and different Linux distributions or boot media options- you may need to troubleshoot and/or try various combinations.

### Some Linux-based distributions

Forensics: Kali Linux ([www.kali.org](http://www.kali.org)). Others include DEFT ([www.deflinux.net](http://www.deflinux.net)) and CAINE ([www.caine-live.net](http://www.caine-live.net)), the latter also includes Windows tools.

Recovery and repair: Trinity Rescue Kit (<http://trinityhome.org>).

### Using a live session

Explore a computer's file systems using a live booted system. Note the difference between the live operating system filesystem, and filesystems on hard drive partition(s) of the investigated computer.

You may need to mount partitions on the investigated computer if the live boot system doesn't do this automatically. Using the desktop GUI to open disk icons may do this, or use the 'mount' command in the command line (described in [Forensic imaging](#) below). Note: This activity doesn't address the forensic need for "write blocking", discussed later.

## Hashing

Hashing algorithms can be used to compute a smaller bit of text from the content a file or drive, that is unique to that file or drive. This therefore provides a useful "fingerprint" or "signature" for digital material. A common use in digital forensics is to verify that a copy is the same as the original, by comparing their hashes, providing the evidential certainty required by forensics.

### Example: Hashing

This example copies a file in Linux terminal, then uses the sha256sum hash utility to compare hashes:

```
$ ls
Digitalforensics.docx

$ cp Digitalforensics.docx DigitalforensicsCopy.docx

$ ls
DigitalforensicsCopy.docx  Digitalforensics.docx

$ sha256sum Digitalforensics.docx
f8b2e7ccac2e4320c0471f481ce80dc41fc7d7cee853ded3979ad664b6d486cd
Digitalforensics.docx

$ shasum DigitalforensicsCopy.docx
f8b2e7ccac2e4320c0471f481ce80dc41fc7d7cee853ded3979ad664b6d486cd
DigitalforensicsCopy.docx
```

Windows: Use the CertUtil command.

## Time stamps

File time stamps are important in digital forensics, for example for establishing “timelines” of computer activities. “MAC” times refer to file **created**, **modified** and **accessed** datetimes.

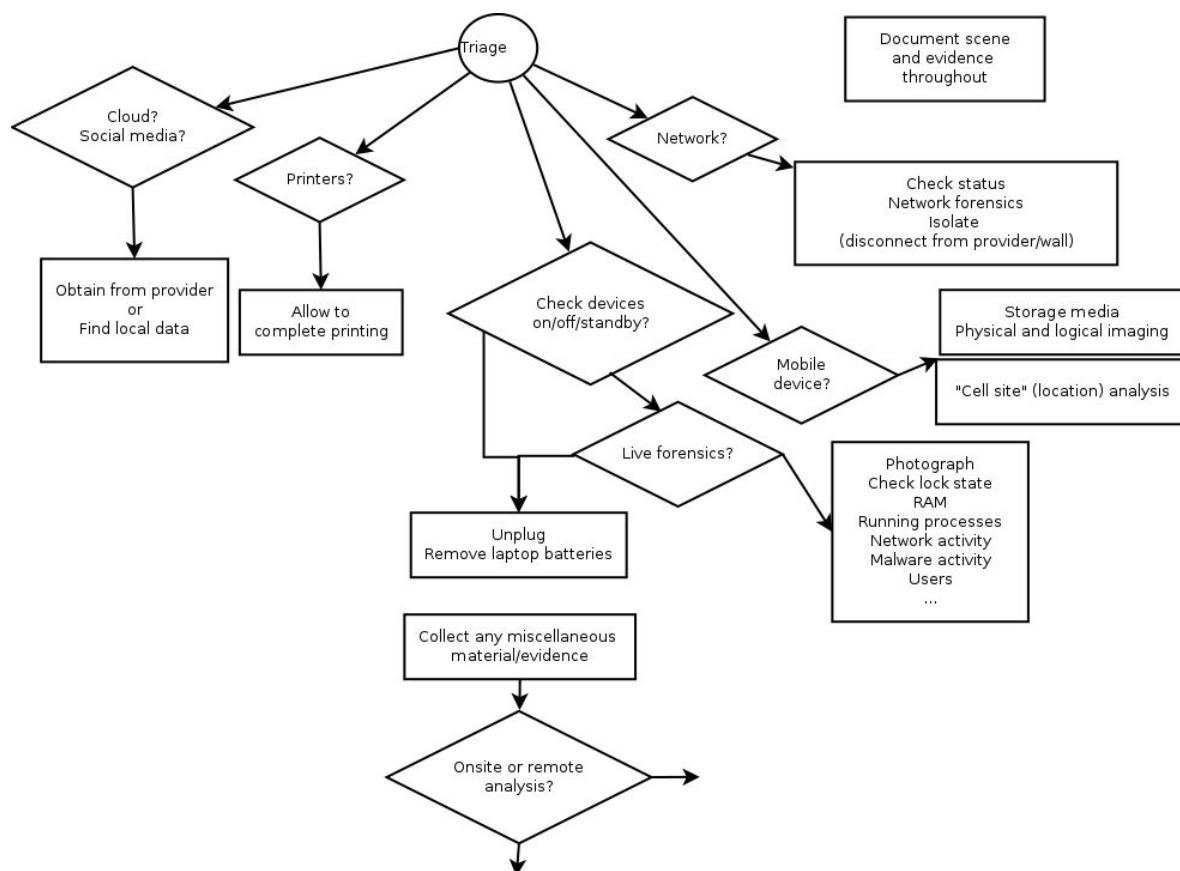
The created time refers to the file on the current medium, i.e. this will update when a file is copied. Accessed time often reflects non-user action, such as an antivirus scan. [TBC:] Copying may also change modified and accessed times, depending on OS/filesystem type [?].

In Linux, use the `stat <filename>` command to view MAC times.

## Evidence acquisition

“**Static**” or “**dead machine**” forensics: Analysis of devices that have been powered down (see also [Digital forensic artefacts](#) below). “**Live**” forensics: More complicated analysis of running devices, incorporating “volatile” or “memory” and “network” forensics. This may be necessary for example if encryption is being used, to collect evidence of ongoing incidents or for critical systems that can’t be shut down (see [Live forensics](#) below). Other specialisms include mobile forensics, cloud computing and social media.

This pseudo-flowchart attempts to show some major activities and decisions. It would be modified according to situation.



( Larger version: <http://www.thebrentc.net/articles/digitalforensics/DigitalForensicsTriage.png> ).

“**Pull the plug**”: If it is decided to switch off a computer for later analysis, this is done by pulling the power cable out. This freezes the computer state for evidence, preventing the tidying up that computers do when shut down properly. The plug is pulled at the computer end, in case there is an Uninterruptible Power Supply (UPS) in the loop that may then trigger normal computer shut down. **Note**: Computers don’t like this; it’s not generally recommended to try.

## Forensic imaging

Digital forensics usually makes forensic images of hard drives for analysis. A simple method is using a live boot system to make a copy or “image” of either a whole computer disk or a partition, saved as a single (usually large) file on an external USB drive.

This needs to ensure “write blocking” is implemented. Write blocking prevents any writing to the source computer, avoiding potential contamination of this evidence. There are expensive hardware devices, or forensic Linux distributions such as Kali have a “forensic mode” that provides software-based write blocking.

The basic steps are as follows (taking contemporaneous notes):

1. Prepare the forensic tools- live boot media with write blocking, external USB, etc.
2. Boot with the live media system.
3. Attach and mount the external USB for storing the image (this needs write access).
4. Compute the hash of the source for later comparison.
5. Take an image of the source (a whole disk or partition), saving to the external USB.
6. Compute and compare the hash of the copy.
7. Unmount media and shutdown.

Later steps:

1. On your forensic workstation, you will probably make “working” copies of the original “master” copy.
2. You will need to mount image files to see the content, and/or use specialised software.

**Linux commands for imaging** (these may require root access, via su or sudo):

**DD** (data duplicator)

This is the archetypal imaging tool. The format is:

```
dd <source> <target>
```

For example:

```
$ dd if=/dev/sdb of=sdb.img
```

Sample output:

```
992802+0 records in  
992802+0 records out
```

DD is also generally useful, for example for making or restoring backups.

Note: It is recommended to use an error-tolerant tool variant for imaging (such as ddrescue), that can handle possible drive errors.

**Related tools:** ddrescue, dcfldd. Commercial tools such as Encase and Forensic Toolkit (FTK) tools handle various aspects of forensics including imaging and image management.

**Warning: Make sure the input and output parameters of dd are correct, otherwise you might mistakenly overwrite a wrong partition and lose data.**



## **Mount**

Attaches a storage medium (or image file) at an access point on the Linux filesystem, i.e.:

```
mount <something> <somewhere> # (run as root)
```

For example:

```
$ mount /dev/sdb1 /mnt
```

allows to view the content of /dev/sdb1 (possibly an external drive) by browsing the /mnt folder.

An image file made of a drive or partition can be similarly mounted, i.e.:

```
$ mount <imagefile> <mountpoint>
```

For example:

```
$ mount image.img /mnt
```

Forensically, media or images for investigation would normally be mounted readonly, using the options:

```
$ mount -o ro,loop <imagefile> <mountpoint>
```

### **Imaging**

Most of these techniques can be practised on any Linux computer (bypassing forensic requirements).

1. Use a small capacity USB flash drive (to take less time).
2. Use dd as above to make an image of a partition on the USB drive to a file, e.g. on your hard drive somewhere.
3. Use the commands as above to mount and view this image.

For Windows, the UnxUtils project usefully provides many Linux commands including dd ( See: <http://unxutils.sourceforge.net/> )

### **Info: Unmounting**

Operating systems may automatically mount drive partitions. If practicing mount commands, you may need to “unmount” these first. Desktop icons may provide “eject” options or the umount command can be used (as root). To see details, use the “manual” help: \$ man umount

**Info: Make your own image files**

An image file with a filesystem can be created directly on Linux (i.e. without using external media). To create a 1.44MB floppy disk sized image (as root):

```
$ dd bs=512 count=2880 if=/dev/zero of=imagefile.img # creates  
image  
$ mkfs.msdos imagefile.img # format to msdos (FAT) filesystem
```

This then needs to be mounted as a “loopback device” as follows:

```
$ mount -o loop imagefile.img /mnt
```

This can now be used like an external media, in this case browsing the /mnt location.

**Link**

<https://untitledfinale.wordpress.com/2007/10/09/create-mount-and-copy-floppy-disks-images-under-linux/>

### Info: Mounting a partition within a full disk image

If you make an image of a whole disk, the offset option will need to be used to mount a specific partition within the full disk image:

```
$ mount -o ro,loop,offset=nnnnnn <imagefile> <mountpoint>
```

To calculate the offset: Inspect the image file using fdisk (as root), note the “sector size” and the “Start” value of the partition. Multiply these to obtain the partition offset. For example:

```
$ fdisk -l sdb.img
```

Shows:

```
Disk sdb.img: 508 MB, 508314624 bytes
14 heads, 18 sectors/track, 3939 cylinders, total 992802 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x1d1f85c8
```

Device	Boot	Start	End	Blocks	Id	System
sdb.img1		<b>2048</b>	992801	495377	b	W95 FAT32

Multiply, e.g.:

```
$ echo $((512 * 2048))
1048576
```

Then mount:

```
$ mount -o ro,loop,offset=1048576 sdb.img /mnt
```

### Reference

Hayden, M. (2010) *Mounting a raw partition file made with dd or dd\_rescue in Linux* [Online]. Available at [https://major.io/2010/12/14/mounting-a-raw-partition-file-made-with-dd-or-dd\\_rescue-in-linux/](https://major.io/2010/12/14/mounting-a-raw-partition-file-made-with-dd-or-dd_rescue-in-linux/)

## Linux, Mac, BSD [draft]

The command line of the Unix operating system “extended family” are similar, but differ particularly in filesystems they use, and how they “mount” filesystems.

### Linux

Linux automounts partitions at /media..., or these can be manually mounted as required, e.g. at /mnt.

### Mac

MacOS automounts at /Volumes/...

Corresponding to the Linux /dev/sdXN naming scheme (e.g. /dev/sda1), Mac uses /dev/diskXsN scheme (e.g. /dev/disk0s1).

Shortcuts to mount from image file into /Volumes/...:

```
hdiutil mount <filename>
```

or

Double-click the .img file

Try:

```
diskutil
```

[TODO]

### BSD

BSD is another unix-based operating system family, including FreeBSD, OpenBSD and NetBSD.

BSD maps disk devices as /dev/ada\* or /dev/da\*. What Linux calls “partitions”, BSD calls “slices”. The equivalent of /dev/sda1 in BSD might be /dev/ada0s1, where ada0 indicates first drive, and s1 indicates the first “slice”.

BSD specifically further divides up these slices into sections, for BSD operating system use, and it calls these sections “partitions”. These are indicated for example as: /dev/ada0s1a, /dev/ada0s1b, etc.

## Netcat

Another imaging technique is copying a drive over the network, using the 'netcat' facility.

### Playing with netcat.

Netcat can transfer any data. For demonstration purposes, we can send a single file from one computer to another (from "source" to "target"). This only works on a local network.

1. Get the IP address of the target computer, using:

```
$ ifconfig # as root
...
```

2. Set the target computer into netcat "listening" mode on a specific "port", directing any input received to the desired output file, for example:

```
$ nc -l -p 6789 -q 10 > DigitalForensics.docx
```

3. Use netcat to send the desired file from the source computer to the listening target computer (referencing the IP and port):

```
$ nc 192.168.1.86 6789 -w 10 < Digitalforensics.docx
```

This activity can be less interestingly practiced on a single computer, using two terminal windows and different locations or filenames.

Netcat for Windows: <https://joncraton.org/blog/46/netcat-for-windows/>

**Warning:** Antivirus programs on organisation computers may alert on attempts to install netcat (due to security concerns).

Another digital forensic use for netcat is in "live" system forensics, where the output of commands on the suspect computer are sent to a forensic computer via netcat.

## Low-level data analysis

Digital forensics often looks at storage media and data at the binary level of the bits and bytes. Forensic programs are useful for this (for example Autopsy and the underlying Sleuth Kit) but it can be done with basic utilities; “Hex viewers” show the numerical representation of digital data using the “hexadecimal” number system, but also try to give a readable representation that shows any actual text “strings”.

### Example: xxd

Using the Linux ‘xxd’ command to view a saved copy of the hacktionlab.org home page shows the location address “offsets”, the hexadecimal and an equivalent text representation (in this case HTML):

```
$ xxd HacktionLab.html | less
# (outputting via the less command provides scrollability)

00000000: 3c21 444f 4354 5950 4520 6874 6d6c 3e0a  <!DOCTYPE html>.
0000010: 3c68 746d 6c20 6c61 6e67 3d22 656e 2220  <html lang="en"
0000020: 6469 723d 226c 7472 2220 636c 6173 733d  dir="ltr" class=
0000030: 2263 6c69 656e 742d 6e6f 6a73 223e 0a3c  "client-nojs">.<
0000040: 6865 6164 3e0a 3c74 6974 6c65 3e48 6163  head>.<title>Hac
0000050: 6b74 696f 6e4c 6162 3a20 6120 6761 7468  ktionLab: a gath
0000060: 6572 696e 6720 616e 6420 776f 726b 696e  ering and workin
0000070: 6720 7072 6f6a 6563 7420 666f 7220 7465  g project for te
0000080: 6368 2d61 6374 6976 6973 7473 2069 6e20  ch-activists in
0000090: 7468 6520 554b 3c2f 7469 746c 653e 0a3c  the UK</title>.<
...

```

### Using xxd

Try use xxd to view a file.

Xxd can also view any data, including a whole drive or partition e.g. /dev/sda, /dev/sdb1.

Windows: Try HxD (available as portable-type app at <https://www.pendrivelabs.com/hxd-portable-hex-editor/>)

This may be combined with commands such as the Linux grep to search for specific strings, and the xxd -s and xxd -l options used to specify start and end points for display

# Undeleting

Deleted data can often be undeleted.

## Undeleting utilities

Experiment with the utilities testdisk and photorec to view/undelete deleted files on a USB flash drive (these utilities work well with FAT32 formats).

## Example: Manual undelete [draft]

On FAT32, deleting only changes the first letter of the filename(s). As proof-of-concept, Linux utilities xxd and dd can be combined to manually undelete a file. For example (using sdd1):

1. Create a file e.g. test.txt (on a FAT32 USB stick, preferably small and clean formatted).
2. For later reference, find and note the location of the filename:

```
$ xxd xxd /dev/sdd1 | grep -i "test"
```

Example output:

```
0002220: 5445 5354 2020 2020 5458 5420 0000 ea92 TEST TXT ...
```

3. To work with the options for dd and xxd below, we need to convert this hexadecimal address [TBC: To decimal showing bytes count?]:

```
$ echo $((0x0002220))
```

Outputs: 8736

4. Delete the file ("fully" delete, e.g. using Shift-Del).

6. Confirm with xxd, filename record has changed:

```
$ xxd -s 8736 /dev/sdd1 | less
```

Shows:

```
0002220: e545 5354 2020 2020 5458 5420 0000 ea92 .EST TXT ...
```

7. Use dd to rewrite the first letter of the filename (1 byte):

```
$ dd of=/dev/sdd1 bs=1 ibs=1 count=1 seek=8736
```

This will wait for user input. Enter a letter to write (i.e. T) and press Return.

8. Confirm successful undeletion, in GUI file explorer and/or with xxd.

## Digital forensic artefacts

Depending on the purpose, an investigation could consider the following using static or “dead” machine forensics:

- Operating system details
- Computer time settings
- Time setting changes
- Malware (should always be checked for)
- Users and user levels
- Users login / logout activity
- Last use (there should be no activity after “seizure”)
- Installed (or previously installed) programs
- Most recently used programs or files
- Hibernation data
- Cached memory (swap or pagefile)
- Traces of external devices or drives used
- Temporary files
- Image “thumbnail” caches
- Traces of “virtual machine” use
- Printer spool or cache files
- Image metadata
- Operating system restore points and “shadow” copies (previous file versions)
- Application programs (browser, mail client, etc) data and logs

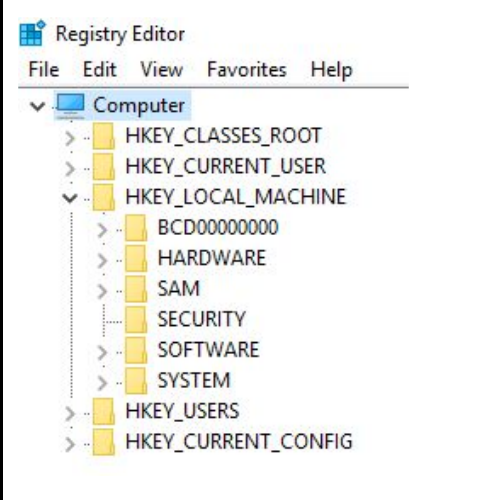
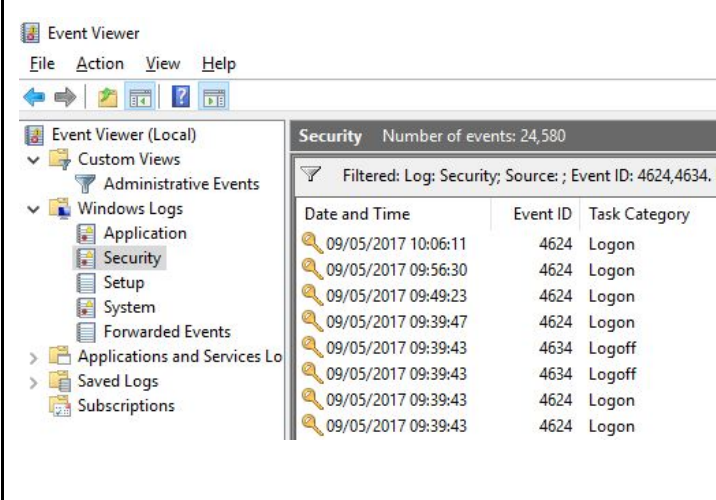
Investigation will possibly include deleted data, and consider hidden data. A common task is building a “timeline”, based on file MAC timestamps, log files, etc. Note that digital forensic evidence may be used in combination with any other evidence e.g. fingerprints, CCTV, etc. as part of a general investigation.

Technical details and tools for forensics are subject to change; the practitioner will need to keep up to date.



## Windows forensics

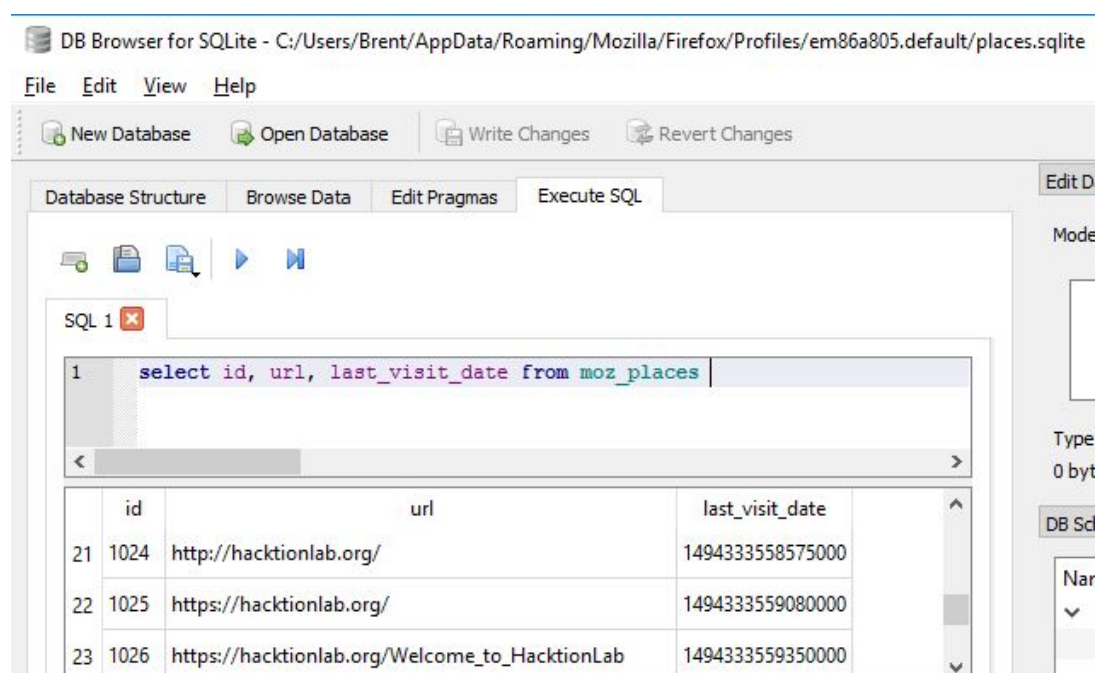
Windows stores much relevant information in “registry keys” contained in specific registry files; this is heavily used in forensics on Windows systems, as well as system “event logs”:

	 <table border="1" data-bbox="965 593 1394 840"> <thead> <tr> <th>Date and Time</th> <th>Event ID</th> <th>Task Category</th> </tr> </thead> <tbody> <tr><td>09/05/2017 10:06:11</td><td>4624</td><td>Logon</td></tr> <tr><td>09/05/2017 09:56:30</td><td>4624</td><td>Logon</td></tr> <tr><td>09/05/2017 09:49:23</td><td>4624</td><td>Logon</td></tr> <tr><td>09/05/2017 09:39:47</td><td>4624</td><td>Logon</td></tr> <tr><td>09/05/2017 09:39:43</td><td>4634</td><td>Logoff</td></tr> <tr><td>09/05/2017 09:39:43</td><td>4634</td><td>Logoff</td></tr> <tr><td>09/05/2017 09:39:43</td><td>4624</td><td>Logon</td></tr> <tr><td>09/05/2017 09:39:43</td><td>4624</td><td>Logon</td></tr> </tbody> </table>	Date and Time	Event ID	Task Category	09/05/2017 10:06:11	4624	Logon	09/05/2017 09:56:30	4624	Logon	09/05/2017 09:49:23	4624	Logon	09/05/2017 09:39:47	4624	Logon	09/05/2017 09:39:43	4634	Logoff	09/05/2017 09:39:43	4634	Logoff	09/05/2017 09:39:43	4624	Logon	09/05/2017 09:39:43	4624	Logon
Date and Time	Event ID	Task Category																										
09/05/2017 10:06:11	4624	Logon																										
09/05/2017 09:56:30	4624	Logon																										
09/05/2017 09:49:23	4624	Logon																										
09/05/2017 09:39:47	4624	Logon																										
09/05/2017 09:39:43	4634	Logoff																										
09/05/2017 09:39:43	4634	Logoff																										
09/05/2017 09:39:43	4624	Logon																										
09/05/2017 09:39:43	4624	Logon																										
<p><i>Windows regedit.exe</i></p>	<p><i>Windows eventvwr.exe</i></p>																											

**Warning:** Changing live registry values can damage the operating system. Export a registry backup first. Digital forensics would normally work from file copies and on a forensic workstation computer.

## Programs / applications

Application programs often store their data in the “sqlite” database format. For example, viewing Firefox’s database table for browsing history, using the “DB Browser for SQLite” PortableApp:



id	url	last_visit_date	
21	1024	http://hacktionlab.org/	1494333558575000
22	1025	https://hacktionlab.org/	1494333559080000
23	1026	https://hacktionlab.org/Welcome_to_HacktionLab	1494333559350000

## Practical links

Some possibly useful programs and links:

- Kali forensic Linux (there are other forensic distributions) : <https://www.kali.org/>
- Kali tools listing : <http://tools.kali.org/tools-listing>
- Autopsy and Sleuth Kit tools : <https://www.sleuthkit.org/autopsy/>
- PortableApps (for Windows) : <http://portableapps.com/>
- CAINE Linux and various Win-Ufo tools : <http://www.caine-live.net/page2/page2.html>
- AccessData FTK Imager Lite :  
<http://accessdata.com/product-download/digital-forensics/ftk-imager-lite-version-3.1.1>
- Windows sysinternals administrator tools :  
<https://technet.microsoft.com/en-gb/sysinternals/bb545021.aspx>
- Windows registry intro :  
<http://www.forensicmag.com/article/2012/02/windows-7-registry-forensics-part-3>
- Identifying time zone (Windows) :  
<http://www.digital-detective.net/manual-identification-of-suspect-computer-time-zone-2/>
- Regripper (Linux tool for Windows registry):  
<https://code.google.com/archive/p/regripper/>
- Reglookup (Linux tool for Windows registry): <http://linux.die.net/man/1/reglookup>  
<http://accessdata.com/product-download/registry-viewer-1.8.1.3> (Windows)
- Windows event log codes : [www.EventID.Net](http://www.EventID.Net)
- Windows system time changes advice :  
<https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4616>
- Python-evtX (Linux) provides evtxdump.py to analyse Windows logs :  
<http://www.williballenthin.com/evtx/>
- Tracking user logon activity :  
<https://blogs.msdn.microsoft.com/ericfitz/2008/08/20/tracking-user-logon-activity-using-logon-events/>
- DB browser for SQLite databases (sqlitebrowser) : <http://sqlitebrowser.org/>
- Libpst providing readpst for Outlook mail files :  
<https://alioth.debian.org/projects/libpst/>
- Pasco tool for Internet Explorer history :  
<https://www.mcafee.com/uk/downloads/free-tools/pasco.aspx>

## Live forensics [dev]

The analysis of running devices, incorporating “volatile” or “memory” and “network” forensics.

TODO: Try Volatility Framework ([www.volatilityfoundation.org/](http://www.volatilityfoundation.org/)).

## Anti-forensics

This is a non-exhaustive list of some techniques and considerations.

### Hidden operating systems etc.

Anonymising, portable operating systems such as Tails ( <https://tails.boum.org/> ) may be used to cover tracks.

“Virtualised” operating systems (running an operating system within another, for example with Virtualbox or VMware) may be used, with the “guest” operating system images stored separately for example on a USB stick, to try hide computer use.

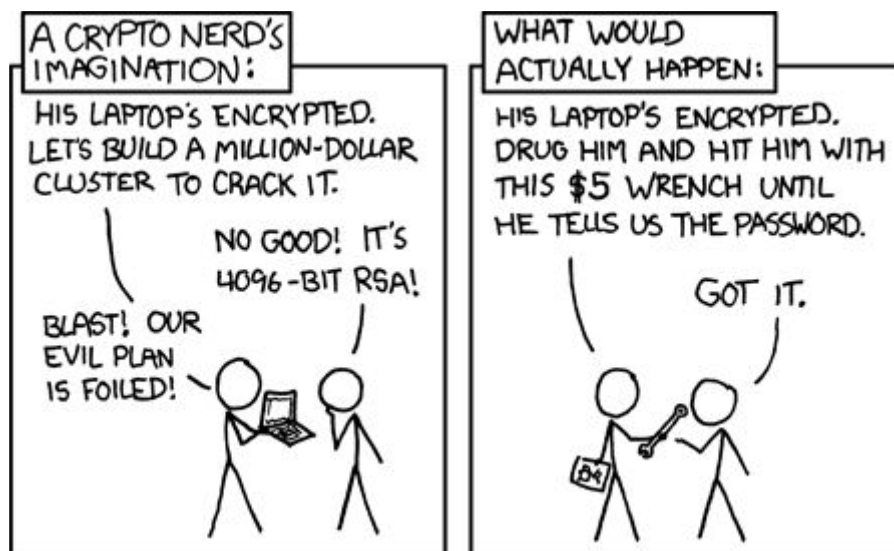
Virtualisation can leave traces on the “host” operating system; virtual network adapters, file associations, etc. Note also that virtualisation has innocuous uses, for example testing.

### Encryption

“Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on. Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it. “ (Snowden, 2013, on [www.theguardian.com](http://www.theguardian.com)).

Infrequent use of encryption may stand out and arouse suspicions. Laws that compel decryption or password disclosure, such as the UK *Regulation of Investigatory Powers Act 2000*, can function as a “rubber-hose cryptanalysis”:

( [https://en.wikipedia.org/wiki/Rubber-hose\\_cryptanalysis](https://en.wikipedia.org/wiki/Rubber-hose_cryptanalysis) )



From <https://xkcd.com/538/>

Programs such as veracrypt (<https://sourceforge.net/projects/veracrypt/>) allow to have hidden, nested encryption drives; the idea being that the outer encryption is a decoy that can be revealed under duress, with deniability of the hidden encryption.

## Steganography

Steganography is hiding data within other data, usually also encrypted. This attempts to hide the existence of the data itself. For example, data can be mixed into an image file without affecting the image quality enough to be visible to the human eye.

### Try steganography

Experiment with the steghide utility on Linux (use jpg image files).

### Example: Weak steganography

As a proof of concept, a “secret” file can simply be appended to the end of an image (following <https://www.ostechnix.com/hidden-files-linux/> ), for example:

```
$ cat image.jpg secret.txt > image2.jpg
```

There are programs that can detect steganography.

## Secure deletion

Secure deletion or “wiping” first overwrites data to be deleted with null or random data to try prevent later undeleting. Secure file deletion utilities include: srm (Linux), shred (Linux), sdelete (Windows) and Eraser (Windows / PortableApps).

DD is also used, especially to overwrite a whole partition or disk. **Warning:** Be Careful with dd to avoid overwriting a wrong partition or drive.

For example:

```
$ dd if=/dev/zero of=/dev/sdb1
# overwrites partition sdb1 with zeros
```

Or, better, but slower:

```
$ dd if=/dev/urandom of=/dev/sdb1
# overwrites partition sdb1 with random characters
```

Depending on paranoia level, repeat, for example:

```
$ for n in 1 2 3; do dd if=/dev/urandom of=/dev/sdb1; done
```

### Dd overwrite a file

To use dd to overwrite a single file, you will first need to get the file length (use: ls -l), then specify this using the bs option to dd, for example:

```
$ dd if=/dev/urandom of=<filename> bs=<filelength> count=1 conv=notrunc
```

Then delete the file itself.

Wiping data as above leaves a characteristic trace (a fill of zeros or random characters) that looks different to a normal use pattern. Sudden wiping activity around the time of an investigation where there hasn't been a routine of doing this can raise suspicion of covering up. It is also very difficult to truly erase all traces of activity across modern operating systems, and file systems such as NTFS and EXT that include “journaling” or file versioning features (Geiger, 2005).

## Link / references

Geiger, M. (2005) 'Evaluating Commercial Counter-Forensic Tools', *Digital Forensic Research Conference (DFRWS)*. New Orleans, 17 - 19 Aug [Online]. Available at [www.dfrws.org/2005/proceedings/geiger\\_couterforensics.pdf](http://www.dfrws.org/2005/proceedings/geiger_couterforensics.pdf)

<https://www.marksanborn.net/howto/wiping-a-hard-drive-with-dd/>

<https://www.marksanborn.net/security/securely-wipe-a-file-with-dd/>

## “Trojan horse” defence

This is arguing a defence that some malware or perhaps another perpetrator committed an alleged crime. This defence will be challenged and evidence sought for or against. Digital forensics needs to check for any malware, and whether this has been active and had a relevant effect.

## Forensic readiness

Forensic readiness means building forensic capability into organisations (or other practice). This aims to appropriately manage potential evidence and prepare for potential investigations, avoiding risks of evidence not being available if needed, or being compromised by standard incident response actions.

Some considerations:

Balancing security, incident investigation and recovery with evidence preservation.

Incident detection.

Evidence management.

Managing devices including mobile devices and “BYOD” (“bring your own device”).

Legal review, consultation and policies for example monitoring arrangements ([ref. ACLU guidelines]).

Disclosure and privacy arrangements.

Audit trails.

Awareness, training and procedures.

## References

Information Assurance Advisory Council (IAAC) (2013) *Digital Evidence, Digital Investigations and E-Disclosure: A Guide to Forensic Readiness for Organisations, Security Advisers and Lawyers*. [Online]. Available at

<http://www.iaac.org.uk/media/1347/iaac-forensic-4th-edition.pdf>

NCSC (2015) *Good Practice Guide Forensic Readiness* [Online]. Available at

[https://www.ncsc.gov.uk/content/files/guidance\\_files/GPG%2018%20-%20Forensic%20Readiness%20-%20Issue%201.2%20-%20Oct%2015%20-%20NCSC%20Web.pdf](https://www.ncsc.gov.uk/content/files/guidance_files/GPG%2018%20-%20Forensic%20Readiness%20-%20Issue%201.2%20-%20Oct%2015%20-%20NCSC%20Web.pdf)

## Fixes for Kali Linux

Some versions of Kali Linux (e.g. 2016.1-i386 and 2017.1-i386) need bugs fixed for the Autopsy and Sleuth Kit tools to work;

```
# Install specific version of sleuthkit
wget --output-document=sleuthkit-4.1.3.tar.gz
https://sourceforge.net/projects/sleuthkit/files/sleuthkit/4.1.3/sleuthkit-4.1.3.tar.gz/download
sha1sum sleuthkit-4.1.3.tar.gz # optional to verify hash
tar xvfz sleuthkit-4.1.3.tar.gz
cd sleuthkit-4.1.3/
./configure
make
make install
rm /usr/bin/srch_strings
cp tools/srchtools/srch_strings /usr/bin

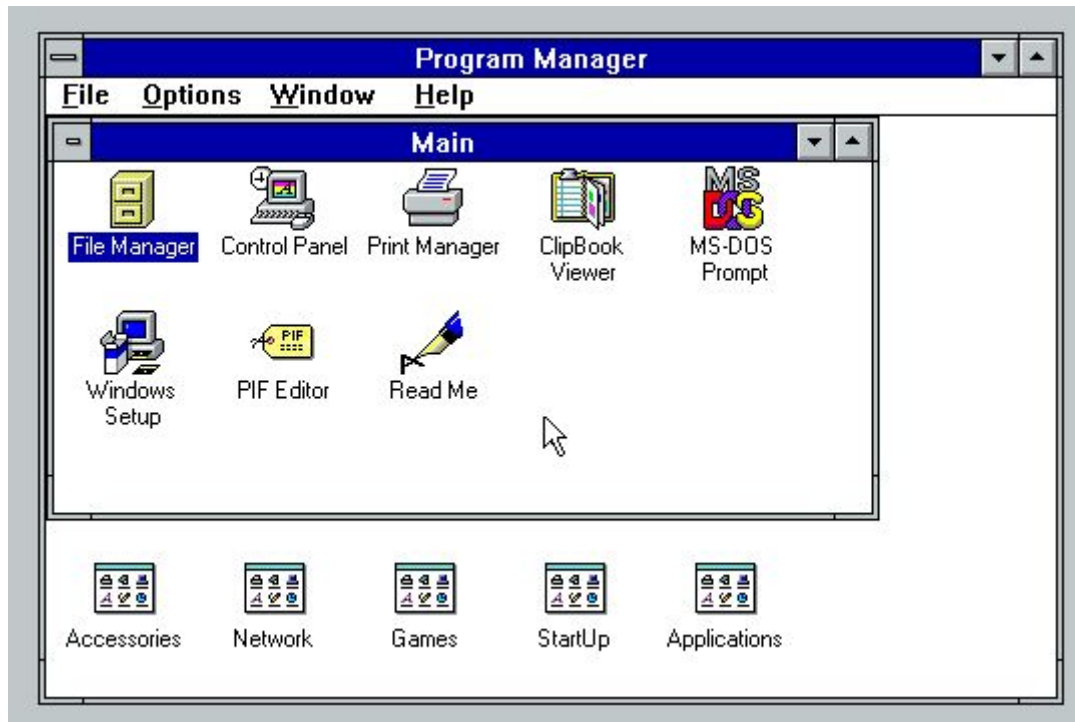
# Set up required shortcuts
ln -s /usr/bin/mactime /usr/bin/mactime-sleuthkit
ln -s /usr/bin/icat /usr/bin/icat-sleuthkit
ln -s /usr/bin/ils /usr/bin/ils-sleuthkit
```

### Links:

- <https://sourceforge.net/p/sleuthkit/mailman/message/34234285/>
- <https://sourceforge.net/projects/sleuthkit/files/sleuthkit/4.1.3/>
- <https://bugs.kali.org/view.php?id=2319>



## Windows 3.11



- Use FAT16 filesystem
- It is a single user system without any login mechanism
- Registered name, company and serial number is in C:\WINDOWS\SERIALNO.INI
- Windows 3.11 runs on top of MSDOS. MSDOS is installed into the DOS folder, and called by C:\COMMAND.COM
- .EXE and .COM files are executables, .INI or .SYS usually configuration, and .BAT files are stored scripts
- AUTOEXEC.BAT runs on system startup
- Windows and its application program files is installed into the C:\WINDOWS
- It doesn't have a specific documents location, users would create folders as required
- FAT16 has only a last modified datetime [?]
- It has a paging file (memory cache) at C:\WINDOWS\WIN386.SWP
- System configuration info is in C:\WINDOWS\SYSTEM.INI
- FAT16 doesn't have other features, such as file 'shortcuts'.

See also: <http://www.informatics.buzdo.com/p560-ms-windows-3-11.htm>

## Workshop plan

- **Introduction**
  - Introductions
  - What is digital forensics? Why learn digital forensics? (2 mins)
    - (law, computing and investigation)
    - Important notes and cautions (2 mins)
      - Discussion: Scenarios and Ethics
  - Discussion: Workshop aims? (Options below) (2 mins)
- **Theory**
  - Key themes: evidence, necessity and proportionality, “cybercrime”
    - See booklet
    - Optional discussion
- **Practical**
  - Overview of technical basics (10 mins)
    - (command line, live booting, disk structures, mounting, imaging)
    - Demo/Practice:
  - Boot into Kali, command line, check disks/partitions, [mount/browse], imaging demo.
    - Questions/comments?
    - Optional demo: low-level view (2 mins)
  - Optional: Practice activities (as above, e.g. using the command line)
- **Anti-forensics**
  - Optional discussion
- **Exercise**
  - Practical digital forensic exercise (30+ mins)
- **Conclusion**
  - Recap
  - Parked topics for later (...)

Kit for participants: Laptop, if participating in practical activities, or participants can just watch demos.

**Note:** As general advice, risk assess your use of any supplied flash drives, downloadable material, etc.

Workshop kit / preparation:

Laptop(s), power supply and extensions, with Kali live boot and/or virtualisation, network optional.

Projector if available, or large printouts: workshop plan, overview, command line help, disk structure example, xxd example, etc.), with stand and pens.

Exercise(s): instructions, images, sample cross-examination, possible solutions.

[Open/close website link].

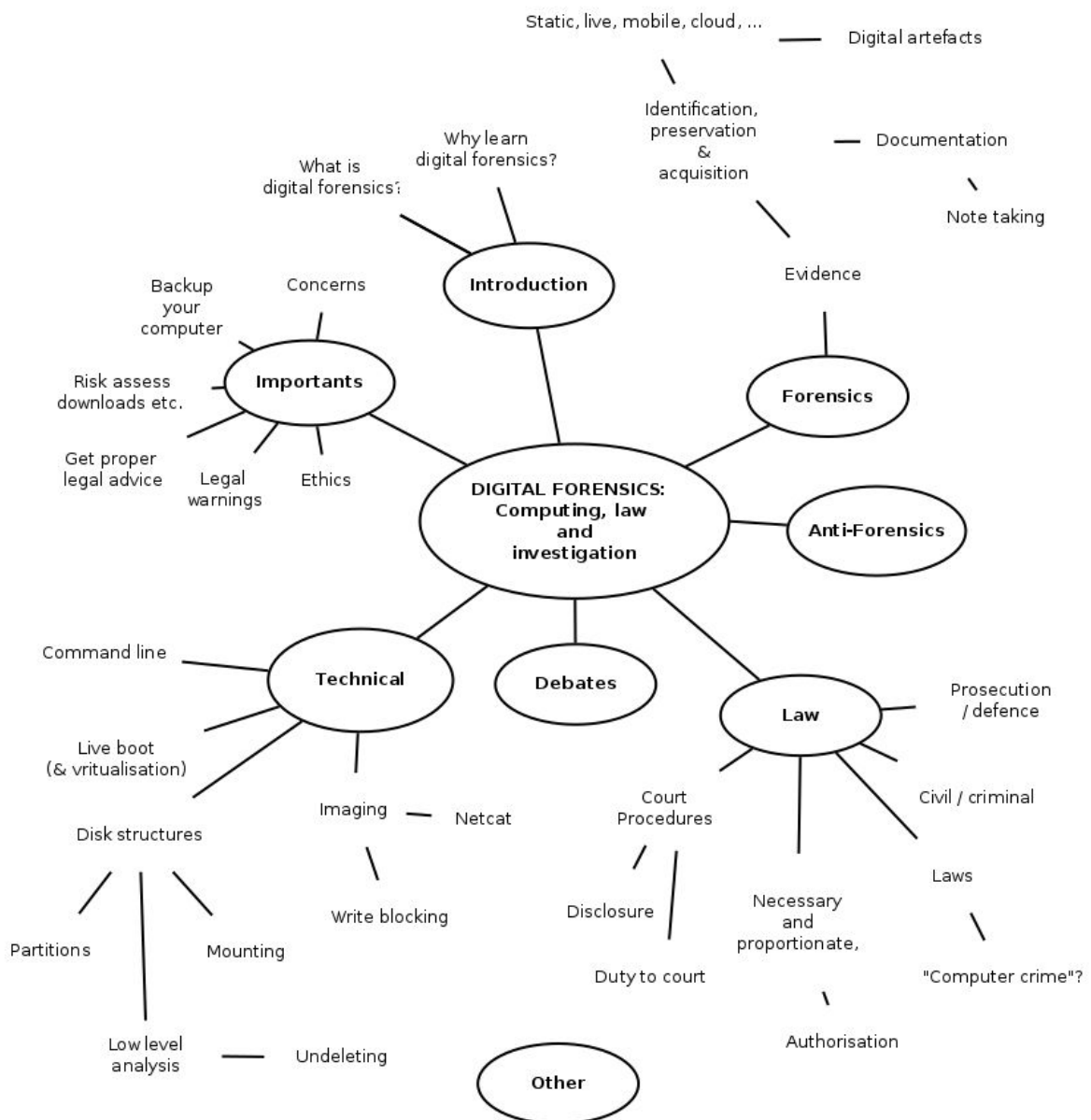
Spare live boot media, small, clean USB flash drives, external DVD drive, floppy disks and drives?

Paper and pens.

Spare computers?

Aluminium foil for faraday shield activities.

## Overview



## Links / further reading

ForensicsWiki. Available at <http://forensicswiki.org>

Hacktionlab (2012) 11. *Hiding & deleting things on your PC*, in *Tech tools for activists* [Online]. Available at [https://hacktionlab.org/upload/1/16/Ttfa\\_insidess\\_v2\\_for\\_print\\_1.pdf](https://hacktionlab.org/upload/1/16/Ttfa_insidess_v2_for_print_1.pdf)

Hoog, A. (2011) *A Geek's Guide to Digital Forensics or How I learned to stop worrying and love the hex editor* [online]. Available at <https://www.youtube.com/watch?v=rPd-HiEvhhw>