**Judicial training**

**Introductory course on cybercrime and electronic evidence for judges and prosecutors**

**Pre-read material on Electronic Evidence and glossary of terms**

# **Introduction**

This pre-read is to prepare delegates, who are attending and participating in the Council of Europe (COE) Introductory Judicial Training course on Cybercrime and Electronic Evidence. The document is substantially based on the COE Electronic Evidence Guide, which was originally prepared under the joint regional project Cybercrime@IPA of the European Union and the Council of Europe (COE) on cooperation against cybercrime under the Instrument of Pre-Accession (IPA). The first edition was published on 18th March 2013 and has since become a popular resource for law enforcement and judicial bodies in a variety of different countries. Some countries have even translated the guide into their domestic languages.The second edition of the Guide is the current basis for materials used in this handout and based on the feedback provided by readers.

This document is designed to prepare delegates for the training course and should be considered as part of the course itself. The materials taught on the course will build upon the learning from this document and will assume that delegates have made themselves familiar with its content. Delegates who arrive at the course without undertaking the pre-read will be at a substantial disadvantage and may not benefit fully from the taught course. In addition to an introduction to the subject of electronic evidence and the descriptions of devices, the pre read includes a glossary of terms, with which delegates should make themselves familiar prior to the training course they are attending. This is also a permanent reference for delegates to retain.

Delegates may wish to avail themselves of further reading before the course. The tools listed below will be beneficial in preparation.

## Further tools

There is a wide range of resources and tools available to complement the Electronic Evidence Guide. For example:

* The Budapest Convention on Cybercrime[[1]](#footnote-1) Parties to the Convention are expected to enact law enforcement powers for securing electronic evidence and for enabling efficient international cooperation. Under Article 14 these powers can be applied to electronic evidence in *any* offence. These powers include:
  + Expedited preservation of data at domestic (Article 16) and international (Article 29) levels, including the partial disclosure of traffic data (Articles 17 and 30);
  + Search and seizure of stored computer data (Article 19);
  + Real-time collection of traffic data and interception of content data at domestic (Articles 20 and 21) and international (Articles 33 and 34) levels;
  + Rapid mutual assistance to access data in foreign jurisdictions (Article 31);
  + Transborder access to data without the need for mutual assistance (Article 32).
* The proposal for law enforcement training strategies prepared under CyberCrime@IPA;
* The judicial training concept prepared by the Council of Europe and the training materials developed under CyberCrime@IPA;
* The typology study on criminal money flows on the internet prepared by MONEYVAL and the Global Project on Cybercrime of the Council of Europe;
* The guidelines for law enforcement/internet service provider cooperation adopted at the Octopus Conference of the Council of Europe in 2008;
* The Octopus Cybercrime Community, a forum linking up the many hundred public and private sector cybercrime experts from all over the world.

These standards and tools are available at www.coe.int/cybercrime.

The following information is essential reading prior to attending the training course.

## What is electronic evidence?

All criminal proceedings depend on evidence to decide the guilt or innocence of an accused or to decide the merits of a case in civil proceedings. Traditionally and historically, evidence has been in a physical form (such as documents or photographs etc.) or the oral testimony of witnesses.

Electronic evidence is derived from electronic devices such as computers and their peripheral apparatus, computer networks, mobile telephones, digital cameras and other portable equipment (including data storage devices), as well as from the Internet. The information it contains does not possess an independent physical form.

However, in many ways, electronic evidence is no different from traditional evidence in that the party introducing it into legal proceedings must be able to demonstrate that it reflects the same set of circumstances and factual information as it did at the time of the offence. In other words, they must be able to show that no changes, deletions, additions or other alterations have (or might have) taken place.

The intangible nature of any data and information stored in electronic form makes it much easier to manipulate and more prone to alteration than traditional forms of evidence. This has created special challenges for the justice system which requires that such data be handled in a special way to ensure the integrity of the evidence it offers.

Given its special characteristics electronic evidence could be defined as:

Any information generated, stored or transmitted in digital form that may later be needed to prove or disprove a fact disputed in legal proceedings.

### Characteristics of electronic evidence

Electronic evidence shares most properties with traditional forms of evidence, but also possesses some unique characteristics:

**It is invisible to the untrained eye**: Electronic evidence is often found in places where only specialists would search or in locations reachable only by means of special tools.

**It is highly volatile**: On some devices and under certain conditions computer memory (and the evidence it contains) can be overwritten (or altered) by the usual functioning or operation of the device. This might be caused, for instance, by a loss of power or where the system needs to lay (or ‘write’) new information over the top of the old due to lack of memory space. Computer memory can also be corrupted or lost through environmental factors such as excessive heat or humidity or through the presence of electromagnetic fields.

**It may be altered or destroyed through normal use**: Computer devices constantly change the state of their memories, be it on user request (“save this document”, “copy this file”) or automatically by the computer operating system (“allocate space for this program”, “temporarily store information to swap it between devices”).

**It can be copied without degradation**: Digital information can be copied indefinitely with each copy exactly the same as the original. This unique attribute means that multiple copies of the evidence can be examined independently and in parallel by different specialists for different reasons without affecting the original.

Like other types of forensic evidence, the correct acquisition and handling of electronic evidence are vital to the outcome of a case. Close attention must be paid to ensure that the general guidelines are followed always:

**Handling by specialists**: Every kind of electronic device has its own specific characteristics that require the correct and appropriate procedures must be applied. One of the greatest risks is the unintentional modification of the evidence. Failure to adhere to approved procedures is likely to lead to formal challenges in court about data integrity that can undermine or invalidate the evidence.

**Rapid evolution of electronic evidence sources:** New technologies are invented and develop very quickly. Consequently, the procedures and techniques to be applied to them also need to be constantly reviewed and updated.

**Use of proper procedures, techniques and tools**: As in more traditional forensic disciplines, digital forensic specialists require special tools and knowledge to undertake their investigations properly. It is imperative that the correct techniques and tools are used for the situations encountered. The procedures must also be auditable and repeatable by other specialists if the information obtained is to have evidential value.

**Admissibility**: Since the goal is to use evidence to prove or disprove disputed facts, electronic evidence must be obtained in compliance with existing legislation and best practice to ensure admissibility at trial.

### Admissibility of electronic evidence

Although the details may differ from jurisdiction to jurisdiction, the following criteria should generally be considered when evaluating electronic evidence for trial:

**Authenticity**: The evidence must establish facts in a way that cannot be disputed and is representative of its original state.

**Completeness**: The analysis of or any opinion based on the evidence must tell the whole story and not be tailored to match a more favourable or desired perspective.

**Reliability**: There must be nothing about the way in which the evidence was collected and subsequently handled that may cast doubt on its authenticity or veracity.

**Believability**: The evidence must be persuasive as to the facts it represents and the finders of fact in the court process must be able to rely on it as the truth.

**Proportionality**: The methods used to gather the evidence must be fair and proportionate to the interests of justice: the prejudice (i.e. the level of intrusion or coercion) caused to the rights of any party should not outweigh the “probative value” of the evidence (i.e. its value as proof).

## Why is it important?

Criminals are predators and the mass use of digital media and Internet has provided new opportunities for them to perpetrate their crimes. They have evolved new strategies for traditional offences by exploiting these new channels of communication and novel categories of crime have evolved. Consequently, it is imperative for all those involved in the legal system to be familiar with the different forms of electronic evidence and to know how to deal with them.

Almost any crime these days is likely to involve an electronic device that has a memory or some form of programming. Even where the crime itself has not used such a device, the actions of the perpetrator may well have been captured or recorded on a CCTV camera or through a Global Positioning System (GPS) device on a phone or in a vehicle. The securing of electronic evidence through digital forensic examination and investigation has become the primary tool in bringing criminals to justice.

The development of the Internet and its applications has led to evidence being found not only on personal computer devices, but also on websites, social networks, in emails and chat rooms. The development of “cloud” computing (where applications and data are stored remotely across national boundaries in non-specific locations) means that it is more important than ever for potential electronic evidence to be processed according to tried and trusted principles and practice.

## Principles of electronic evidence

The following principles, from the COE electronic evidence guide, are provided to guide readers when dealing with electronic evidence. Much has changed in the world of technology in the decade since these principles were formulated so they have been amended to meet the challenges of today’s operational environment.

**Each country should consider its own legal documents and regulations when interpreting the measures proposed in this document.** This is such an important point, it will be repeated often!

### Principle 1 – Data Integrity

### No action taken should materially change any data, electronic device or media which may subsequently be used as evidence in court.

* Electronic devices and data must not be changed, either in relation to hardware or software. The person in charge of a crime scene or for collecting the evidence is responsible for maintaining the integrity of the material recovered and for ensuring the forensic chain of custody. Subsequent custodians of the devices and/or data must assume that responsibility.
* When data is accessed on a “live” computer system this must be done in the manner that causes the least impact on the data and by a person qualified to do so. Principles 2 to 5 apply if this course of action is found to be necessary.

### Principle 2 – Audit Trail

**A record of all actions taken when handling electronic evidence should be created and preserved so that they can be subsequently audited. An independent third party should not only be able to repeat those actions, but also to achieve the same result.**

* It is imperative to record accurately all activity at the scene to enable a third party to reconstruct the first responder’s actions if necessary. All activity relating to the search, seizure, access, storage or transfer of electronic evidence must be fully documented, preserved and available for review.
* Any subsequent action related to the processing and examination of electronic evidence should also be amenable to audit in the same way.

### Principle 3 – Specialist Support

**If it is expected that electronic evidence may be found during a planned operation, the person in charge of the operation should notify specialists/external advisers in time and to arrange their presence if possible.**

* For investigations involving search and seizure of electronic evidence it is always desirable to involve electronic evidence specialists wherever possible. All such specialists, either from within the organisation or as external contractors, should have the appropriate and objectively verifiable knowledge to deal with electronic evidence properly. Such a specialist should have:
  + Sufficient specialist expertise and experience in the field;
  + Sufficient knowledge and skills in conducting investigations;
  + Sufficient knowledge of the matter at hand;
  + Sufficient legal knowledge;
  + Appropriate communication skills (for both oral and written explanations);
  + Sufficient and appropriate language skills;
  + Appropriate authorisation and/or legal justification for his/her involvement in the activity.

### Principle 4 – Appropriate Training

**First responders must have the necessary and appropriate training to be able to search for and seize electronic evidence if no specialists are available at the scene.**

* For those circumstances where only a first responder is available to collect electronic evidence and/or access original data held on an electronic device or digital storage media, s/he must be trained to do so according to legally sanctioned procedures and to be able to explain and justify the relevance and implications of his/her actions.

### Principle 5 - Legality

**The person and agency in charge of the case are responsible for ensuring that the law, the evidential safeguards and the general forensic and procedural principles are followed to the letter.**

# Sources of evidence

The variation in devices containing electronic evidence increases almost daily. The following list of potential sources of evidence is not exhaustive, but contains examples of those most commonly found.

A computer system will be made up of several different components that are likely to include:

* An external case housing **circuit boards, microprocessors**, hard drives, **memory,** and connections for other devices;
* A monitor or other display device;
* A keyboard;
* A mouse;
* Externally connected drives;
* Peripheral devices;
* Software.

Computer systems can come in many different forms including desktops, laptops, tower computers, rack-mounted systems, minicomputers, and, mainframe computers. Other devices will commonly connect to these systems including printers, scanners, routers, external hard drives and other storage devices as well as docking stations (that allow multiple connections to be made).

Note the definition of “computer system” and “computer data” used in the Budapest Convention on Cybercrime:

*Article 1 – Definitions*

*For the purposes of this Convention:*

1. *"computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;*
2. *"computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;*

This definition covers tablets, smart phones and other devices described below.

**

Images of computer systems[[2]](#footnote-2)

### Storage devices

Storage devices also come in many shapes and sizes and vary in the manner in which they store and keep data. The following section provides details of some of these devices and their capabilities.

#### Hard disk drives and solid state disks

Hard disk drives (HDD) are the main storage devices within computer systems. They consist of a circuit board, data and power connections. Inside the hard disk drive there are magnetically-charged ceramic, metal or glass platters (i.e. plates or disks) that rotate at high speed. An arm travels across the surface of the platter like in old fashioned record players and ‘writes’ the data to the disck. It is not unusual to discover separate hard disk drives during a search that are not connected to or installed in a computer system. Usually a hard disk drive in desk top computers will measure 3.5 inches (8.9 cm) across and 2.5 inches (6.35 cm) across laptops.

Solid state disks (SSD) have a different structure to hard disks and are becoming more popular. Instead of storing data on platters, solid state disks store data using microchips and have no moving parts. As such they are less likely to be damaged when dropped or knocked and offer faster access to the data.



Photographs of different types of internal storage[[3]](#footnote-3)

#### Removable media

Compact Disk (CD), Digital Video Disk[[4]](#footnote-4) (DVD) and Blu-ray Disks (BD) are typically used for storage of large video or audio files. They may, however, also hold large quantities of other kinds of data that can be of evidential value. Although they look very similar, the storage capacities vary greatly.

****

Photographs of different types of removable optical storage[[5]](#footnote-5)

#### Memory cards

Memory cards, also known as flash cards, are also devices for storing digital information. They are used in devices such as digital cameras, mobile phones, laptop computers, music players and games consoles. They retain data without power and can store huge amounts of data while being easy to conceal.

****

Types of memory cards[[6]](#footnote-6)

#### USB data storage devices

Universal Serial Bus (USB) is the name given to a set of rules or ‘protocol’ used for communication, connection and power supply for devices that connected to computers. The range of devices using this protocol has grown enormously since it was introduced in the 1990s. Some examples of the more usual USB devices are shown below.

****



Images of common USB devices[[7]](#footnote-7)

However, not all devices are what they seem. Here are just a few of the ways in which USB storage devices can be disguised. It is important for anyone considering electronic evidence to be vigilant and aware of the possible novelty.





Images of unusual USB devices[[8]](#footnote-8)

#### Data storage tape disks

Data stored on tape is more likely to be encountered in a business rather than a domestic setting. The most common type used now is the ‘Linear Tape-Open’ (LTO) technology developed in the 1990s as an open-format[[9]](#footnote-9) standard. Tapes are normally used for backup and therefore may be useful in cases where an historical analysis is required or where the original computer is not available.

****Images of data storage tape devices[[10]](#footnote-10)

#### Peripheral devices

Peripherals are devices that are not an integral part of the computer, but connect to it to increase its range of functions. Examples of peripheral devices are: scanners; printers; tape drives; webcams; loudspeakers; microphones; calculators; fax machines; answering machines; and card readers. Many of these devices have their own data storage capacity and may be relevant to particular types of investigation (for example, the presence of a card reader may be relevant in a credit card cloning investigation). Here are some images of just a few of the types of peripherals that might be encountered:



Images of Peripheral Devices[[11]](#footnote-11)

### Tablet devices

A tablet computer is a device that is operated by touching the screen rather than using a keyboard or mouse. It is normally larger than a mobile phone or **Personal Digital Assistant** (PDA). Tablets may store data in the form of a hard disk or flash memory, but , increasingly, user-generated data are stored in the cloud. Tablets have become very popular in recent years. They run their own operating systems and are often connected to the Internet via a Wireless Local Area Network (**WLAN**), Third Generation Mobile Telecommunications **(3G*)*** (now slowly becoming Fourth Generation or 4G) or Long Term Evolution (**LTE**)[[12]](#footnote-12)networks.



Photographs of tablet devices[[13]](#footnote-13)

### Mobile telephones

The time when a telephone was used simply for making and receiving calls is long past. Nowadays, mobile or ‘cell’ phones are used for many other tasks: sending and receiving text or multimedia messages; accessing the Internet and email; playing games; listening to music; and, taking photographs. Many modern mobile phones are really computers, although their connectivity requires them to be handled in a somewhat different manner. It is important to note that different phones have different capabilities and the way they connect (their ‘connection interfaces’) can require specialist equipment in order to capture evidence.



Images of Mobile Phones[[14]](#footnote-14)

### Photo and video recording

#### Digital cameras

Digital cameras take still or video photographs in the form of thousands of small dots of light called pixels. Most modern digital cameras can also record sound as well as pictures. Digital cameras can store thousands of images on small “memory cards” (see 2.1.1.3 above) or on the camera itself. For investigations involving photographs it may be possible to prove which camera took a specific photograph because certain metadata are often stored with the image[[15]](#footnote-15). Examples of common types of digital camera are shown below, along with some cameras disguised as other devices.



Images of Digital Cameras[[16]](#footnote-16)

#### Digital video cameras

A digital video camera also often stores its images on removable media, but can also record to a hard disk contained within the camera itself. In some cases these cameras look very similar to digital still cameras (bearing in mind that digital still cameras can usually also take video and a digital video camera can take still photographs). Some examples of video cameras are shown below.

****

Images of Digital Video Cameras[[17]](#footnote-17)

#### Video recorders

Video recorders are usually found in the domestic setting and used to record TV programmes or other locally based activity. They are also used to playback prerecorded films, music and other data. The Video Home System (VHS) recorders were prominent from the 1970s until overtaken by digital versions. VHS was recorded and played back using large cassette tapes that may still be found under some circumstances. Certain kinds of optical discs were also produced, but did not become mainstream. Instead, the Digital Versatile Disk (DVD) became the standard. DVDs and their later evolution, Blu-ray discs, are still used today, but some modern video recorders store their recording on built-in hard drives. Where CCTV is present, images the cameras may be recorded in any of these formats.

****

Video Recording Formats[[18]](#footnote-18)

#### Digital audio recorders

Digital audio recorders are small handheld devices used to record sound on a memory chip to play the recording back. They come in various capacities in terms of maximum recording time and quality. Some recorders have a USB capability that allows the recordings to be uploaded to a computer and may have associated speech recognition software allowing for the creation of automatic draft transcripts.



Images of Digital Audio Recorders[[19]](#footnote-19)

#### CCTV cameras

Closed Circuit Television (CCTV) cameras are used by companies, governments and private individuals. CCTV cameras may be deployed continually or to monitor a particular activity. In some countries they have become a tool for surveillance in public places monitoring traffic or crowd flows, detecting public disorder or criminal activity. Some CCTV cameras record images onto storage media while others are only used for live monitoring. They can also be motion activated and operate in low light or under infrared conditions. They should always be considered as a potential source of electronic evidence wherever they are at or near a crime scene. Some examples of how CCTV cameras may look like are shown below.



Images of CCTV Cameras[[20]](#footnote-20)

### Portable media players

Portable media players such as iPods or **MP3[[21]](#footnote-21)** players store and play digital media. These can include music and other audio, photographs or video as well as documents and other types of file. Once again, these devices have many similarities with computers. Some of these devices use removable flash storage while others have large hard disks capable of storing many thousands of files. Some examples of portable media players are provided below.



Images of Portable Media Players[[22]](#footnote-22)

### Video games consoles

Video games consoles have existed since the early 1970s, but have developed greatly over the years. These devices use onboard or removable storage that allows the users not only to play games, but also to visit websites and to store and play videos, photos and music. For this reason, they should never be overlooked as sources of electronic evidence even if they seem innocuous at first sight. Major console producers include Sony, Nintendo and Microsoft and these companies currently hold the majority of the market for consoles and games.

  
Images of Video Games Consoles[[23]](#footnote-23)

### Potential evidence on these devices

Computer hardware and software, as well as the networks and systems to which a device is connected, can hold important data that have been created either automatically by the device itself or by the user. User-generated data would include documents, photos, image files, e-mails and their attachments, databases and financial information. Computer generated data would include the Internet browsing history, chat logs, event logs and data about other services, computers and networks to which the device has been connected.

## Computer networks

When two or more computers are linked by data cables or by wireless connectivity a ‘network’ is established. Computers in a network are able to share data and other resources between them and will often be connected to additional hardware components that extend their scope and the functions available. Computer networks can be limited such as those found in the home (e.g. where members of a family establish a network sharing an Internet modem) or as extensive as those used by major corporations or governments linking hundreds or even thousands of computers together.

**Local Area Network (LAN) –** A Local Area Network is a computer network covering a limited ‘local’ area like a home, an office, or a group of buildings (such as a school). Defining characteristic of LANs include the much higher speed they can achieve for transferring data between computers on the network, the limited geographic range and the fact that they do not need to rent lines from telecommunications companies.

**Wide Area Network (WAN)** – A Wide Area Network is a computer network that covers a broader area and will include any network that crosses metropolitan, regional, or national boundaries. The term implies a network that uses routers[[24]](#footnote-24) and public communications links.

Contrast these with personal area networks (PANs), campus area networks (CANs), or metropolitan area networks (MANs) which are usually limited to a room, building, campus or specific metropolitan area respectively. The largest and most well-known example of a WAN is the Internet.

Some of the terminology and devices that may be encountered when dealing with networks are:

**Port** – There are two types of ports: computer or hardware ports and network or internet ports. A computer port is a connection point between a computer and another device where information comes in and out (examples include USB, Ethernet and parallel ports by which devices can be attached). A network port is located in the software at the point where the software connects to internet or network services. A common analogy would be the doors and windows to a building. Each port is allocated a different number in computer programming. The number identifies the port’s role and function and is set according to common standards.

**Bandwidth** – Like the diameter of a pipe, the size of the bandwidth indicates the maximum volume of information that can be carried along a phone line, cable line, satellite feed etc. The greater the bandwidth, the faster the potential speed for downloading and uploading data.

**Media Access Control (MAC) address** – The MAC address is a unique reference code assigned by the manufacturer to most network adaptors or network interface cards (NICs). MAC addresses function as an address on a network so that devices can be identified and the appropriate data can be forwarded to it.

**CoE 72-74.tiffNetwork Attached Storage (NAS)** – A NAS is similar to an external hard-drive with the difference that it provides storage space for a whole network rather than just a single PC. NAS can often offer a lot more than just data storage. A NAS can be used as an automatic downloading server (e.g. uTorrent) and even as a small webserver. Many NAS devices house more than one hard drive and offer ‘RAID’ functionality.

A so-called ‘Redundant Array of Independent Disks’ (**RAID**) is a way of arranging the storage of data (a data ‘configuration’) using multiple disk drives. Data is stored across the individual disks to ensure the best level of performance and/or data reliability. The operating system will access the RAID as though it were a single hard disk. The access is controlled and coordinated either by software or by a hardware RAID controller. Standalone RAIDs are commonly found in network configurations and may contain huge amounts of electronic evidence.



Images of NAS with RAID[[25]](#footnote-25)

**Network Interface Controller (NIC)** – is a circuit board or card installed in a computer that allows it to connect to a network.



Network Interface Controllers[[26]](#footnote-26)

**Network Hub** – A network hub or concentrator is a device for connecting multiple computers or Internet devices together so that they act together as a single part or ‘segment’ of a network. All computers in this segment are able to communicate with each other A hub transmits any data received from the network and broadcasts it to all the other devices connected to it. For an investigator it can be hard to distinguish between hubs and switches because they basically look the same, but hubs have been largely replaced by network switches. The main difference is that a hub broadcasts all packets to all ports while a switch sends it only to the target port.

****

A Network Hub[[27]](#footnote-27)

**Network Switch** – A network switchis very similar to a hub. Switches are mainly used to connect groups of network devices to each other. In contrast to hubs they use internally stored databases to remember which MAC address has used which port of the switch. This allows a switch to route data packets to a specific device rather than to all devices.



A Network Switch[[28]](#footnote-28)

**Router** – A router is like a sorter in a post room. It is a device that identifies the destination to which a parcel or packet of data is addressed and then sends that packet on to the next point in the network nearest to where it needs to go. Although a router must be located at the gateway between networks it does not necessarily have to be linked to the Internet. Routers are commonly used in the home to connect a house to a broadband connection. In such a situation it will often serve multiple purposes acting as a switch, access point, firewall, router and gateway all together.

****

Image of a Router[[29]](#footnote-29)

**Server** – A server is a computer or device that provides information and/or services to other computers on a network. Given the right software, any network-connected computer can be configured as a server. In most cases, a server will be a dedicated powerful computer designed to be “always available”. One computer server can run several services (e.g. web server, email server, file server, print server etc.). In business it often makes sense to run different services on different machines for reasons of security and to minimise the impact of any failure.

****

Images of Servers[[30]](#footnote-30)

**Firewall** – A firewall is a hardware device or software service that is used to increase the security of a network by preventing unauthorised access. For instance a firewall may be configured (set up) to detect and block any attempt to enter a network using multiple ports except for those ports that have been configured to allow incoming traffic. In homes, it is more common to find a software firewall, but in business settings the investigator is more likely to come across hardware firewalls.



Images of Hardware Firewalls[[31]](#footnote-31)

**Wireless Access Point** – Wireless Access Points connect Wireless LAN devices to the rest to the network. In every WLAN infrastructure an access point is necessary whenever there are more than two devices. Modern routers can often function as an Access Point. A computer’s NIC or even a mobile phone can also be configured to act as an Access Point.



Images of Access Points[[32]](#footnote-32)

While the network devices listed above can be standalone devices as shown in the photographs, it is very likely that a single device will serve multiple purposes. Routers in the home often function as a modem, firewall, switch and access point and a Networked Attached Storage (NAS) system may also serve as a Virtual Private Network , E-Mail and Webserver with switching as well as access point capabilities.

**Potential Evidence on These Devices**

Computer hardware and software, as well as the networks and systems to which a device is connected, can hold important data that have been created either automatically by the device itself or by the user. User-generated data would include documents, photos, image files, e-mails and their attachments, databases and financial information. Computer generated data would include the Internet browsing history, chat logs, event logs and data about other services, computers and networks to which the device has been connected.

# Glossary[[33]](#footnote-33)

**24/7 RealMedia:** is a technology company headquartered in [New York City](http://en.wikipedia.org/wiki/New_York_City) specializing in Digital Marketing. It provides digital marketing solutions for publishers, advertisers and agencies globally. It was formerly listed as "TFSM" on the NASDAQ stock exchange.

**3G networks: 3G** or **3rd generation mobile telecommunications** is a generation of standards for mobile phones and mobile telecommunication services fulfilling the **International Mobile Telecommunications-2000 (IMT-2000)** specifications by the International Telecommunication Union.Application services include wide-area wireless voice telephone, mobile Internet access, video calls and mobile TV, all in a mobile environment.

**Access Control Lists (ACLs):** is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects. Each entry in a typical ACL specifies a subject and an operation.

**Access token:** is an object encapsulating the security descriptor of a process. Attached to a process, a security descriptor identifies the owner of the object (in this case, the process) and [ACLs](http://en.wikipedia.org/wiki/Access_Control_List) that specify access rights allowed or denied to the owner of the object. While a token is used to represent only the security information, it is technically free-form and can enclose any data. The access token is used by Windows when the process or thread tries to interact with objects whose security descriptors enforce access control (*securable objects*).

**Acquisition:** a process referred to as Imaging. The duplicate is created using a hard-drive duplicator or software imaging tools such as [DCFLdd](http://en.wikipedia.org/w/index.php?title=DCFLdd&action=edit&redlink=1), [IXimager](http://en.wikipedia.org/w/index.php?title=IXimager&action=edit&redlink=1), [Guymager](http://en.wikipedia.org/w/index.php?title=Guymager&action=edit&redlink=1), TrueBack, [EnCase](http://en.wikipedia.org/wiki/EnCase), [FTK](http://en.wikipedia.org/wiki/FTK) Imager or FDAS. The original drive is then returned to secure storage to prevent tampering. The acquired image is verified by using the SHA-1 or MD5 hash functions. At critical points throughout the analysis, the media is verified again, known as "hashing", to ensure that the evidence is still in its original state. In corporate environments seeking civil or internal charges, such steps are generally overlooked due to the time required to perform them.

**Active data:** Files and folders that reside in the IT system storage units that are accessible and visible to the users in an immediate and direct manner by the means of the operating system’s tools.

**AdBrite:** is an online advertising network, based in San Francisco, California, which was founded by Philip J. Kaplan and Gidon Wise in 2002. Originally founded as Marketbanker.com, the site was relaunched as AdBrite in 2004 and now serves advertisements on hundreds of thousands of sites, according to their published statistics.

**AdCenter: Microsoft adCenter** (formerly **MSN adCenter**), is the division of the Microsoft Network (MSN) responsible for MSN's advertising services. Microsoft adCenter provides [pay per click](http://en.wikipedia.org/wiki/Pay_per_click) advertisements. This is a service aimed at people who want to advertise a product. Microsoft also has a (still in beta) service for webmasters who want to monetize on their site: Microsoft pubCenter.

**AfriNIC** (**African Network Information Center**): is the regional Internet registry (RIR) for Africa.

**Amazon S3** (**Simple Storage Service**): is an online storage web service offered by Amazon Web Services. Amazon S3 provides storage through web services interfaces (REST, SOAP, and BitTorrent). Amazon launched S3, its first publicly-available web service, in the United States in March 2006 and in Europe in November 2007.

**API:** An **application programming interface** is a specification intended to be used as an interface by software components to communicate with each other. An API may include specifications for [routines](http://en.wikipedia.org/wiki/Subroutine), [data structures](http://en.wikipedia.org/wiki/Data_structure), [object classes](http://en.wikipedia.org/wiki/Class_%28computer_programming%29), and variables. An API specification can take many forms, including an International Standard such as [POSIX](http://en.wikipedia.org/wiki/POSIX) or vendor documentation such as the Microsoft [Windows API](http://en.wikipedia.org/wiki/Windows_API), or the [libraries](http://en.wikipedia.org/wiki/Library_%28computing%29) of a programming language, e.g. [Standard Template Library](http://en.wikipedia.org/wiki/Standard_Template_Library) in [C++](http://en.wikipedia.org/wiki/C%2B%2B) or [Java API](http://en.wikipedia.org/wiki/Java_API).

**APNIC (Asia Pacific Network Information Centre):** is the [regional Internet registry](http://en.wikipedia.org/wiki/Regional_Internet_registry) for the [Asia Pacific](http://en.wikipedia.org/wiki/Asia_Pacific) region. APNIC provides number resource allocation and registration services that support the global operation of the Internet. It is a not-for-profit, membership-based organization whose members include Internet Service Providers, National Internet Registries, and similar organizations.

**ARIN (American Registry for Internet Numbers):** is the [Regional Internet Registry](http://en.wikipedia.org/wiki/Regional_Internet_Registry) (RIR) for [Canada](http://en.wikipedia.org/wiki/Canada), many Caribbean and North Atlantic islands, and the [United States](http://en.wikipedia.org/wiki/United_States). ARIN manages the distribution of Internet number resources, including [IPv4](http://en.wikipedia.org/wiki/IPv4) and [IPv6](http://en.wikipedia.org/wiki/IPv6) address space and [AS numbers](http://en.wikipedia.org/wiki/Autonomous_system_%28Internet%29).

**Assistant (PDA):** They come in many forms and sizes and usually have storage capability built in in the form of hard disks or flash memory. They have become very popular in recent years and may be useful sources of electronic evidence as they run their own operation systems and are often connected to the internet via **WLAN**, **3G** or **LTE** networks.

**ATM:** An automatic teller machine (ATM), is a computerized telecommunications device that provides the [clients](http://en.wikipedia.org/wiki/Customer) of a [financial institution](http://en.wikipedia.org/wiki/Financial_institution) with access to [financial transactions](http://en.wikipedia.org/wiki/Financial_transaction) in a public space without the need for a cashier, human clerk or [bank teller](http://en.wikipedia.org/wiki/Bank_teller) (from Wikipedia)

**Autonomous System:** is a collection of connected [Internet Protocol](http://en.wikipedia.org/wiki/Internet_Protocol) (IP) [routing](http://en.wikipedia.org/wiki/Routing) prefixes under the control of one or more network operators that presents a common, clearly defined [routing policy](http://en.wikipedia.org/wiki/Routing_policy) to the Internet.

**Azure:** Microsoft Windows Azure Platform is a Microsoft [cloud computing](http://en.wikipedia.org/wiki/Cloud_computing) [platform](http://en.wikipedia.org/wiki/Platform_%28computing%29) used to build, host and scale [web applications](http://en.wikipedia.org/wiki/Web_application) through Microsoft data centers. Azure is classified as [platform as a service](http://en.wikipedia.org/wiki/Platform_as_a_service) and forms part of Microsoft's cloud computing strategy, along with its [software as a service](http://en.wikipedia.org/wiki/Software_as_a_service) offering, [Microsoft Online Services](http://en.wikipedia.org/wiki/Microsoft_Online_Services). The platform consists of various on-demand services hosted in Microsoft data centers and commoditized through three product brands. These are [Windows Azure](http://en.wikipedia.org/wiki/Windows_Azure) (an operating system providing scalable compute and storage facilities), [SQL Azure](http://en.wikipedia.org/wiki/SQL_Azure) (a cloud-based, scale-out version of [SQL Server](http://en.wikipedia.org/wiki/Microsoft_SQL_Server)) and Windows Azure [AppFabric](http://en.wikipedia.org/wiki/AppFabric) (a collection of services supporting applications both in the cloud and on premise). Microsoft has announced free Ingress for all the customers of Azure from 1 July 2011.

**Backup:** A copy taken of all information held on a computer in case something goes wrong with the original copy.

**Biometric scanners:** a device connected to a computer system that recognizes physical characteristics of an individual (e.g., fingerprint, voice, retina).

**BIOS:** Basic Input Output System. The set of routines stored in read-only memory that enable a computer to start the operating system and to communicate with the various devices in the system such as disk drives, keyboard, monitor, printer, and communication ports.

**Bit:** A **bit** (a contraction of **binary digit**) is the [basic capacity](http://en.wikipedia.org/wiki/Units_of_information) of [information](http://en.wikipedia.org/wiki/Information) in [computing](http://en.wikipedia.org/wiki/Computing) and [telecommunications](http://en.wikipedia.org/wiki/Telecommunication); a bit represents either 1 or 0 (one or zero) only. The representation may be implemented, in a variety of systems, by means of a two state device. In [computing](http://en.wikipedia.org/wiki/Computing), a bit can also be defined as a [variable](http://en.wikipedia.org/wiki/Variable_%28computer_science%29) or computed quantity that can have only two possible [values](http://en.wikipedia.org/wiki/Value_%28computer_science%29). These two values are often interpreted as [binary digits](http://en.wikipedia.org/wiki/Binary_notation) and are usually denoted by the [numerical digits](http://en.wikipedia.org/wiki/Numerical_digit) 0 and 1. The two values can also be interpreted as [logical values](http://en.wikipedia.org/wiki/Truth_value) (*true*/*false*, *yes*/*no*), algebraic [signs](http://en.wikipedia.org/wiki/Signed_number) (*+*/*−*), activation states (*on*/*off*), or any other two-valued attribute. The correspondence between these values and the physical states of the underlying [storage](http://en.wikipedia.org/wiki/Data_storage_device) or [device](http://en.wikipedia.org/wiki/Computing_device) is a matter of convention, and different assignments may be used even within the same device or [program](http://en.wikipedia.org/wiki/Computer_program). The length of a binary number may be referred to as its "[bit-length](http://en.wikipedia.org/wiki/Bit-length)."

**Bluetooth:** A telecommunications industry specification that describes how mobile phones, computers, and PDAs can easily interconnect with each other and with home and business phones and computers using a short-range wireless connection. Bluetooth requires that a low-cost transceiver chip be included in each device.

**Blu-ray Disc (BD):** is an [optical disc](http://en.wikipedia.org/wiki/Optical_disc) [storage](http://en.wikipedia.org/wiki/Data_storage_device) medium designed to supersede the [DVD](http://en.wikipedia.org/wiki/DVD) format. The plastic disc is 120 mm in diameter and 1.2 mm thick, the same size as [DVDs](http://en.wikipedia.org/wiki/DVD) and [CDs](http://en.wikipedia.org/wiki/CD). Blu-ray Discs contain 25 [GB](http://en.wikipedia.org/wiki/Gigabyte) per layer, with dual layer discs (50 GB) being the norm for feature-length video discs. Triple layer discs (100 GB) and quadruple layers (128 GB) are available for *BD-XL* re-writer drives.

**Capturing data:** Capturing data means to copy data from a computer system or electronic media and store them on an external storage media before verifying the integrity of the data where possible (e.g. not possible for capturing RAM). Capturing data can also be possible for network data. In this context on machine in the network is used to capture the network packets and store their information to a file (e.g. in PCAP format).

**CentralOps:** CentralOps is a website offering investigative lookup opportunities like a domain dossier, email dossier, whois lookups, etc. These services can provide information about IP-addresses, domains and email addresses. The website is run by Hexillion is a privately-held company based in the USA. Its’ address is: http://centralops.net

**Chat logs:** is an archive of transcripts from [online chat](http://en.wikipedia.org/wiki/Online_chat) and [instant messaging](http://en.wikipedia.org/wiki/Instant_messaging) conversations. Many chat or IM applications allow for the client-side archiving of online chat conversations, while a subset of chat or IM clients (i.e., Google Talk and [Yahoo! Messenger](http://en.wikipedia.org/wiki/Yahoo%21_Messenger) 11 Beta) allow for the saving of chat archives on a server for future retrieval. The latter trend has been adopted by the applications' vendors because of the decreasing cost of web server hard drive space.

**CIDR notation:** is a compact specification of an [Internet Protocol address](http://en.wikipedia.org/wiki/IP_address) and its associated routing prefix. [Classless Inter-Domain Routing](http://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing) (CIDR) is an [Internet Protocol](http://en.wikipedia.org/wiki/Internet_Protocol) (IP) address allocation and route aggregation methodology[[1]](http://en.wikipedia.org/wiki/CIDR_notation#cite_note-0) used within the [Internet](http://en.wikipedia.org/wiki/Internet) addressing architecture that replaced the [IPv4](http://en.wikipedia.org/wiki/IPv4) [classful network](http://en.wikipedia.org/wiki/Classful_network) organization of the IP address space. It is used also for [IPv6](http://en.wikipedia.org/wiki/IPv6) networking, the next generation of the IP addressing architecture.

**Circuit boards:** A thin plate with chips, devices and other electronic components installed on the plate (also referred to as the printed circuit board).

**Closed Circuit Television (CCTV):** They are used by companies, governments and individuals for security and may provide evidence that certain activities have or have not taken place.

**Cloud:** Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[…]

**CMOS:** Complementary metal-oxide semiconductor. Semiconductor technology used in the transistors that are manufactured into most of today's computer microchips. It commonly holds the BIOS preferences of the computer through power off with the aid of a battery (adapted from).

**Compact Disk (CD):** Optical disc 12cm in diameter used for storing binary information. Its formatted capacity is between 640-700 Mb and was primarily used to store audio. When used for storing generic data it is called CD-ROM.

**Computer Memory:** Memory is the electronic holding place for instructions and data that a computer’s microprocessor can reach quickly. RAM is located on one or more microchips installed in a computer.

**Computer Networks:** consists of connections between two or more computers that are linked by data cables or by wireless connectivity. These computers are able to share data and other resources between them. They often have other hardware components to enable the scope of activities required of the network.

**Cookie:** Cookies are small files that the internet server downloads onto the hard drive of the user’s computer. These files contain specific information that identifies the user (for example, through passwords and lists of websites visited).

**CPU:** Central processing unit. The computational and control unit of a computer. Located inside a computer, it is the "brain" that performs all arithmetic, logic, and control functions in a computer.

**Cracker:** A Cracker is a person that enters into a system without authorisation with the intention of causing some form of damage or to make beneficial gain.

**Cybercrime:** refers to any crime that involves a [computer](http://en.wikipedia.org/wiki/Computer) and a [network](http://en.wikipedia.org/wiki/Computer_network). The computer may have been used in the commission of a crime, or it may be the target.

**Cybersquatter:** A Cybersquatter is a person that reserves or buys domain names with the intention of selling them to interested companies in the future.

**DAT (Digital Audio Tape):** Digital audio tape used for storing media on *back-up* systems.

**Data storage devices:** A **data storage device** is a device for [recording](http://en.wikipedia.org/wiki/Recording) (storing) [information](http://en.wikipedia.org/wiki/Information) (data). Recording can be done using virtually any form of [energy](http://en.wikipedia.org/wiki/Energy), spanning from manual muscle power in [handwriting](http://en.wikipedia.org/wiki/Handwriting), to acoustic vibrations in [phonographic](http://en.wikipedia.org/wiki/Phonograph) recording, to electromagnetic energy modulating [magnetic tape](http://en.wikipedia.org/wiki/Magnetic_tape) and [optical discs](http://en.wikipedia.org/wiki/Optical_disc).

**DATABASE:** Structured collection of data that can be accessed in many ways. Common database programs are: Dbase, Paradox, Access. Uses: various including – address links, invoicing information, etc.

**Dead box forensics:** Dead box forensics is one part of computer forensics which is a branch of digital forensic science pertaining to legal evidence found in computers. Computer forensics deals with the examination of computer systems in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts that might become evidence in a trial. Dead box forensics follow this aim but is only focused on storage media in computer systems that are in a turned off state.

**Deleted data:** Files and folders that existed previously on the computer as active data but since have been deleted by the operating system or the end-user. Deleted data will remain in the storage unit until they are overwritten by another file.

**Desktops:** The term has been adopted as an adjective to distinguish office appliances (such as photocopiers and printers) which can be fitted on top of a desk, from larger equipment covering its own area on the floor. Desktop may also refer to [Desktop computer](http://en.wikipedia.org/wiki/Desktop_computer), a personal computer designed to fit on a desk

**Digital Forensics:** Digital Forensics is a branch of forensic science related to the acquisition, processing, analysis and reporting of evidence that is stored on computer systems, digital devices and other storage media with the aim of admissibility in court.

**Digital media:** is a form of electronic media where data are stored in digital (as opposed to analogue) form. It can refer to the technical aspect of storage and transmission (e.g. hard disk drives or computer networking) of information or to the "end product", such as digital video, augmented reality or digital art.

**Digital photography:** Digital photography is a form of photography that uses an array of light sensitive sensors to capture the image focused by the lens, (from Wikipedia)

**Digital Video Disk (DVD):** Digital Versatile (video) Disc. Presently the natural successor of the CD for the reproduction of quality sound and image.

**DIGITAL VIDEO**: Video captured, manipulated and stored in a digital format.

**Digitalisation:** To store electronic information as a chain of “ones” and “zeros”. Due to the fact that as many “zeros” as “ones” can be easily represented by 2 voltaic levels in electronic media, the binary numbering system is widely used in the digital IT world.

**Diskette Proprietary tools:** IT applications that have been developed expressly in keeping with the functionalities and the operation of the company that utilises it and that, in general, are not available for purchase on the open market.

**Diskette:** Form of media storage, becoming less frequently used, that consists of a circular piece of magnetic material within a plastic case / covering.

**DNS:** Domain Name System (DNS). Transforms the name of a domain, for example www.cybex.es, into the IP address where the server that you are looking for is situated.

**Docking stations:** A device to which a portable computer (e.g., laptop, notebook) can be attached for use as a desktop computer, usually having a connector for externally connected devices such as hard drives, scanners, keyboards, monitors, and printers.

**Domain name:** The **Domain Name System** (**DNS**) is a hierarchical distributed naming system for computers, services, or any resource connected to the [Internet](http://en.wikipedia.org/wiki/Internet) or a [private network](http://en.wikipedia.org/wiki/Private_network). It associates various information with [domain names](http://en.wikipedia.org/wiki/Domain_name) assigned to each of the participating entities. A **Domain Name Service** resolves queries for [domain names](http://en.wikipedia.org/wiki/Domain_name) (which are easier to understand and utilize when accessing the internet) into [IP addresses](http://en.wikipedia.org/wiki/IP_address) for the purpose of locating computer services and devices worldwide. An often-used analogy to explain the Domain Name System is that it serves as the [phone book](http://en.wikipedia.org/wiki/Telephone_directory) for the Internet by translating human-friendly computer [hostnames](http://en.wikipedia.org/wiki/Hostname) into [IP addresses](http://en.wikipedia.org/wiki/IP_address). For example, the domain name [www.example.com](http://en.wikipedia.org/wiki/Example.com) translates to the addresses 192.0.43.10 ([IPv4](http://en.wikipedia.org/wiki/IPv4)) and 2620:0:2d0:200::10 ([IPv6](http://en.wikipedia.org/wiki/IPv6)).

**DomainTools:** DomainTools, LLC provides a directory of domain name [Whois](http://en.wikipedia.org/wiki/Whois) ownership records that serves as a comprehensive snapshot of past and present domain name registration and ownership records that span more than a decade of Internet history. In addition to Whois data, DomainTools offers a set of research tools that helps individuals and organizations discover and monitor everything about a domain name. DomainTools is also known for offering advanced semantic name suggestion technology, patented Reverse [IP](http://en.wikipedia.org/wiki/IP_address) technology, and incorporating millions of screenshots into a combined screenshot history view of how a website looks now and how it used to look like in the past.

**Dongle:** is a small piece of hardware that plugs into an electrical connector on a computer and serves as an electronic "key" for a piece of software; the program will run only when the dongle is plugged in. The term "dongle" was originally used to refer only to software-protection dongles; however, currently "dongle" is often used to refer to any small piece of hardware that plugs into a computer. This article is limited in scope to dongles used for the purpose of copy protection or authentication of software to be used on that system.

**Drive duplicators:** A device for fast copying (duplicating) of different storage media, e.g., hard disks or CDs.

**DropBox:** is a file hosting service operated by Dropbox, Inc. that offers cloud storage, file synchronization, and client software.

**Dynamic Host Configuration Protocol (DHCP):** is a protocol used to automatically assign a pool of IP addresses to a group of devices.

**Electronic evidence:** Electronic evidence is information generated, stored or transmitted using electronic devices that may be relied upon in court. To guarantee that the evidence is accepted in court, it is necessary to obtain the information following very well defined processes using specialised personnel and operating within an adequate legal framework.

**E-mail virus:** Viruses cannot travel in e-mail messages because they only use a 7 bit format to transfer text. The only way that they can travel is by binary files that are sent as attachments with the text message. It is recommended to check these files with an anti-virus before opening.

**Email:** The exchange of computer-stored messages by telecommunication

**Encryption:** Method of scrambling and encoding data. Used to convert plain text into ciphertext (by using a mathematical parameter called cryptographic key) in order to prevent anyone but the intended recipient from reading that data.

**Environmental data:** Refers, as a whole, to the data that is not active on the IT system. Environmental data includes: Data found in unused or unassigned areas, Data found in the “Slack” file space and File data that has been deleted that is not visible using the operating system tools.

**Event logs:** Event Logs are the logfiles saved by the Windows operating systems. Usually there are several Event Logs auditing a variety of events from different services of Windows. The creation of certain Event Logs is turned on by default but can be disabled by the user. The default storage location for Windows XP machines is: C:\Windows\system32\config\\*.evt, for Windows Vista/7 machines it is: C:\Windows\system32\Winevt\\*.evtx

**EXIF metadata:** Exchangeable image file format (Exif) is a standard that specifies the formats for images, sound, and ancillary tags used by digital cameras (including smartphones), scanners and other systems handling image and sound files recorded by digital cameras. Typically there is a lot of information to find in the EXIF metadata, e.g. time, date and place of when and where a photograph has been taken and which camera model with which configuration was used.

**EXT4:** or **fourth extended filesystem** is a journaling file system for Linux, developed as the successor to EXT3.

**External hard drives:** External hard drives are a kind of external storage media. Modern external hard drives consist of a chassis, that offers connectivity via USB, Firewire, eSATA and/or Thunderbolt, and a regular 2,5” or 3,5” hard disk or SSD that is residing inside the chassis. Typically external hard drives can store a larger amount of data compared to USB thumbdrives or SD cards.

**Faraday isolation bags:** A dimensionless unit of electric charge quantity, equal to approximately 6.02 x 10 electric charge carriers. This is equivalent to one mole, also known as Avogadro´s constant. Faraday isolation bags are used to prevent mobile phones and devices from connecting to communication signals

**FAT (File Allocation Table**): is the name of a computer [file system](http://en.wikipedia.org/wiki/File_system) architecture and a family of industry standard file systems utilizing it. The FAT file system is technically relatively simple yet robust. It offers reasonably good performance even in light-weight implementations and is therefore widely adopted and supported by virtually all existing operating systems for personal computers. This makes it a well-suited format for data exchange between computers and devices of almost any type and age from the early 1980s up to the present.

**File extension:** File label usually 3 characters in length, preceded by a decimal point, that identifies the format of the data file or the application used to modify it.

**FireBug:** integrates with Firefox to put a wealth of development tools while browsing. It allows the user to edit, debug, and monitor CSS, HTML and JavaScript live in any web page.

**FireWire:** A high-speed serial bus that allows for the connection of up to 63 devices. Widelz used for downloading video from digital camcorders to the computer.

**Flash cards:** are devices for storing digital information. They are often used in many electronic devices such as digital cameras, mobile phones, laptop computers, music players and games consoles. They are able to retain data without power and come in a variety of capacities, meaning they can store huge amounts of data while being easy to hide from view.

**Forensic Boot-DVDs:** Forensic Boot-DVDs are DVDs that are bootable and contain an operating system containing software to perform digital forensics tasks. Besides just offering the forensic tools these Boot-DVDs take measures to prevent unintended write operations to any of the attached storage media.

**FQDN (Fully Qualified Domain Name):** sometimes also referred as an *absolute domain name*, is a [domain name](http://en.wikipedia.org/wiki/Domain_name) that specifies its exact location in the tree hierarchy of the [Domain Name System](http://en.wikipedia.org/wiki/Domain_Name_System) (DNS). It specifies all domain levels, including the [top-level domain](http://en.wikipedia.org/wiki/Top-level_domain) and the root zone. A fully qualified domain name is distinguished by its unambiguity; it can only be interpreted one way.

**Fragmented data:** Fragmented data is active data that has been divided and stored in different physical locations on the hard disk.

**FTK Imager:** FTK Imager is a multi-purpose software by Access Data Inc. It is free of charge and is capable of imaging, verifying, converting and mounting hard-discs and image files. FTK Imager can be downloaded at the following website: http://accessdata.com/support/adownloads

**FTP (File Transfer Protocol):** Protocol of the internet that allows transfer of files / data between computers connected via the internet.

**Google AdSense:** is a program run by [Google Inc.](http://en.wikipedia.org/wiki/Google_Inc.) that allows publishers in the Google Network of content sites to serve automatic text, image, video, and rich media adverts that are targeted to site content and audience. These adverts are administered, sorted, and maintained by Google, and they can generate revenue on either a [per-click](http://en.wikipedia.org/wiki/Cost_Per_Click) or [per-impression](http://en.wikipedia.org/wiki/Cost_Per_Impression) basis.

**GPS:** The GPS (Global Positioning System) is a "constellation" of 24 well-spaced satellites that orbit the Earth and make it possible for people with ground receivers to pinpoint their geographic location. The location accuracy is anywhere from 100m to 10m for most equipment. GPS devices can provide information on previous travel via destination information, way points, and routes.

**Hacker:** Person that has a thorough knowledge of the functionality of computers and networks that enables them to take advantage of the errors and failures in security of said systems.

**Hard disk:** Metal disk covered with a ferromagnetic burning layer. Making an analogy with a vinyl disc, the flat sides of the disc are the burning layer, the arm of the turntable is the laser arm and the needle on the turntable arm is the laser beam that reads / writes the information. A user can write, delete or re-write on magnetic disks as with audio tape.

**Hard drives:** Hard drives are the major storage device within computer systems. They consist of a circuit board, data and power connections, along with internal magnectically charged, ceramic, metal or glass platters that store the data. It is not unusual to discover hard drives that are not connected to or installed in a computer system.

**Hardware:** The physical components that make up a computer system such as the keyboard, monitor and mouse.

**Hoax:** Term used to define false rumours, especially about non-existent viruses spread over the network. Sometimes they are very successful and cause as much damage as a real virus.

**Hosting providers:** An **Internet hosting service** is a service that runs [Internet](http://en.wikipedia.org/wiki/Internet) servers, allowing organizations and individuals to serve content to the Internet. There are various levels of service and various kinds of services offered. A common kind of hosting is [web hosting](http://en.wikipedia.org/wiki/Web_hosting_service). Most hosting providers offer a combined variety of services. [Web hosting services](http://en.wikipedia.org/wiki/Web_hosting_services) also offer [e-mail hosting service](http://en.wikipedia.org/wiki/E-mail_hosting_service), for example. [DNS hosting service](http://en.wikipedia.org/wiki/DNS_hosting_service) is usually bundled with [domain name registration](http://en.wikipedia.org/wiki/Domain_name_registrar).

**HTML code (Hypertext Markup Language):** Language used for writing documents for web servers. HTML is an application from ISO Standard 8879:1986.

**HTTP (Hypertext Transfer Protocol):** HTTP is a protocol with the necessary agility and velocity to distribute and handle multimedia information systems over the internet. A characteristic of HTTP is the independence in the visualisation and representation of the data, allowing systems to be constructed independently of the development of new advances in the representation of data.

**HTTPs:** Secure HTTP protocol. The 2 principal characteristics are the coding and authentication. By means of the coding, the content of the communication of the server to the third party is concealed. The authentication allows users know that the server is bonafide with the use of certificated signatures by Certification of Authority.

**Forensic copy:** An exact copy (bit by bit) of the unit of storage of an IT system used in a forensic investigation.

**Hubs:** A place of convergence in a network where data arrives from one or more directions and is forwarded out in one or more other directions. It usually works as a multiport repeater by generating a number of identical outputs from a single input (output=input). A hub may include a switch of some kind (adapted from).

**I ROM memory:** ROM stands for *Read-Only Memory*. The memory of the semiconductor that cannot be overwritten and maintains stored information intact, including in the case of loss of power supply. ROM is used to storing the system configuration or the programme from the boot-up of the computer.

**ICQ:** is an [instant messaging](http://en.wikipedia.org/wiki/Instant_messaging) [computer program](http://en.wikipedia.org/wiki/Computer_program), which was first developed and popularized by the [Israeli](http://en.wikipedia.org/wiki/Israel) company [Mirabilis](http://en.wikipedia.org/wiki/Mirabilis_%28company%29), then bought by [America Online](http://en.wikipedia.org/wiki/AOL), and since April 2010 owned by [Mail.ru Group](http://en.wikipedia.org/wiki/Digital_Sky_Technologies). The name *ICQ* is a [homophone](http://en.wikipedia.org/wiki/Homophone) for the phrase "I seek you". This is an adaptation of the [Morse code](http://en.wikipedia.org/wiki/Morse_code) callout "[CQ](http://en.wikipedia.org/wiki/CQ_%28call%29)", which means "calling any station".

**IMAP:** Internet Message Access Protocol. An Internet service based on a standardized protocol for retrieving and/or accessing e-mail messages from the mail server (i.e., IMAP server).

**Infrared:** Infrared wireless technology is used for short- and medium-range communications and control in a variety of applications (e.g., wireless local area networks, links between notebooks and desktop computers, cordless modems, intrusion detectors). Infrared refers to energy in the region of the electromagnetic radiation spectrum at wavelengths longer than those of visible light, but shorter than those of radio waves.

**Instrument of Pre-Accession:** The Instrument for Pre-Accession Assistance (IPA) is the financial instrument for the European Union (EU) pre-accession process for the period 2007-2013. Assistance is provided on the basis of the European Partnerships of the potential candidates and the Accession Partnerships of the candidate countries, which means the Western Balkan countries, Turkey and Iceland. The IPA is intended as a flexible instrument and therefore provides assistance which depends on the progress made by the beneficiary countries and their needs as shown in the Commission’s evaluations and strategy papers.

**Interface “Gnome”:** Is the core [user interface](http://en.wikipedia.org/wiki/User_interface) of the [GNOME](http://en.wikipedia.org/wiki/GNOME) [desktop environment](http://en.wikipedia.org/wiki/Desktop_environment) used by a variety of different Linux distributions. It provides basic functionality like switching between [windows](http://en.wikipedia.org/wiki/Window_%28computing%29) and launching applications. It replaces [GNOME Panel](http://en.wikipedia.org/wiki/GNOME_Panel)and other software components from GNOME 2 to offer a user experience that breaks from the previous model of [desktop metaphor](http://en.wikipedia.org/wiki/Desktop_metaphor), used in earlier versions of GNOME.

**Internet access:** is the means by which individual [terminals](http://en.wikipedia.org/wiki/Computer_terminal), [computers](http://en.wikipedia.org/wiki/Computers), [mobile devices](http://en.wikipedia.org/wiki/Mobile_devices), and [local area networks](http://en.wikipedia.org/wiki/Local_Area_networks) are connected to the global [Internet](http://en.wikipedia.org/wiki/Internet). Internet access is usually sold by [Internet Service Providers](http://en.wikipedia.org/wiki/Internet_Service_Providers) (ISPs) that use many different technologies offering a wide range of [data rates](http://en.wikipedia.org/wiki/Data_rates) to the end user.

**Internet Assigned Numbers Authority** (**IANA**): is the entity that oversees global [IP address](http://en.wikipedia.org/wiki/IP_address) allocation, [autonomous system](http://en.wikipedia.org/wiki/Autonomous_system_%28Internet%29) number allocation, [root zone](http://en.wikipedia.org/wiki/DNS_root_zone) management in the [Domain Name System](http://en.wikipedia.org/wiki/Domain_Name_System) (DNS), [media types](http://en.wikipedia.org/wiki/Internet_media_type), and other [Internet Protocol](http://en.wikipedia.org/wiki/Internet_Protocol)-related symbols and numbers. IANA is a department operated by the [Internet Corporation for Assigned Names and Numbers](http://en.wikipedia.org/wiki/Internet_Corporation_for_Assigned_Names_and_Numbers), also known as ICANN.

**Internet browsing history:** Software that is designed to browse websites like Apple Safari, Google Chrome, Microsoft Internet Explorer, Mozilla Firefox, etc often save histories of websites that were visited by the users of a computer system. The main purpose of these history logfiles or databases is to allow the user to easily choose websites that were visited recently or very often. For forensic examiners the internet browsing history saved by the browsers can be a valuable source for finding evidence.

**Internet Service Provider (ISP):** is an organization that provides access to the [Internet](http://en.wikipedia.org/wiki/Internet). Internet service providers can be either [community-owned](http://en.wikipedia.org/wiki/Community-owned) and [non-profit](http://en.wikipedia.org/wiki/Non-profit), or [privately owned](http://en.wikipedia.org/wiki/Privately_owned) and [for-profit](http://en.wikipedia.org/wiki/For-profit).

**Internet:** Global network of data based on TCP/IP protocol that are utilised to interconnect computers and, as such, the transport of diverse services, the most popular being e-mail, web and FTP services.

**IP address:** Chain of 4 numbers separated by decimal points that are used to represent and identify a computer on the internet. ISP’s assign IPs automatically when we connect to the internet.

**ISP (Internet Service Provider):** Organisation that provides connection to the internet for computers that are dedicated lines or switches. A profit making entity that as well as providing access to the internet for individuals and / or legal entities, can offer services such as web hosting, web-design consultancy, integration of websites and intranets, etc.

**IT system:** An information system (IS) - or application landscape - is any combination of [information technology](http://en.wikipedia.org/wiki/Information_technology) and people's activities that support operations, management and decision making. In a very broad sense, the term information system is frequently used to refer to the interaction between people, processes, data and technology. In this sense, the term is used to refer not only to the [information and communication technology](http://en.wikipedia.org/wiki/Information_and_communication_technology) (ICT) that an organization uses, but also to the way in which people interact with this technology in support of business processes.

**JAVA:** Java is a language oriented to objects and developed by Sun Microsystems. It shares similarities with C, C++ and Objective C. Basing itself on other object oriented languages, Java utilises the best parts of the others and eliminates the least effective points. The principal objective of Java was to make a language that had the capacity to be executed in a secure way across the internet (although the code was maliciously written). This characteristic requires the elimination of many C and C++ uses and constructions. The most important is that no pointers exist. In Java, the program cannot arbitrarily access memory addresses.

**LACNIC (Latin America and Caribbean Network Information Centre**): is the [Regional Internet Registry](http://en.wikipedia.org/wiki/Regional_Internet_Registry) for the [Latin American](http://en.wikipedia.org/wiki/Latin_America) and [Caribbean](http://en.wikipedia.org/wiki/Caribbean) regions. LACNIC provides number resource allocation and registration services that support the global operation of the Internet. It is a not-for-profit, membership-based organisation whose members include Internet Service Providers, and similar organisations.

**LAN:** Local Area Network. A common name for the networking technologies standardized by the IEEE (Institute of Electrical and Electronics Engineers).

**LAN CONFIGURATION:** LAN topology such as Ethernet or token ring, or MAC addresses such as Ethernet address (MAC: Medium Access Control, a part of the data link layer in the OSI seven layer model).

**Linux:** is a [Unix-like](http://en.wikipedia.org/wiki/Unix-like) computer [operating system](http://en.wikipedia.org/wiki/Operating_system) assembled under the model of [free and open source software](http://en.wikipedia.org/wiki/Free_and_open_source_software) development and distribution. The defining component of Linux is the [Linux kernel](http://en.wikipedia.org/wiki/Linux_kernel), an [operating system kernel](http://en.wikipedia.org/wiki/Operating_system_kernel) first released 5 October 1991 by [Linus Torvalds](http://en.wikipedia.org/wiki/Linus_Torvalds).

**Live computer system:** A Live computer system is a computer system that is powered on.

**Live data forensics:** Live data forensics is one part of computer forensics which is a branch of digital forensic science pertaining to legal evidence found in computers. Computer forensics deals with the examination of computer systems in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts that might become evidence in a trial. Live data forensics follow this aim but is only focused on computer systems that are powered on. The main purpose is to acquire volatile data that would otherwise get lost if the computer system is turned off or would be overwritten if the computer system will stay turned on for a longer period.

**Log:** Register of determined events generated by the operating system, or application, about a given period of time. Logs can be used by external auditors for registering / reconstructing the use of the computer or application.

**LTE networks:** LTE Advanced is a [mobile communication standard](http://en.wikipedia.org/wiki/List_of_mobile_phone_standards), formally submitted as a candidate [4G](http://en.wikipedia.org/wiki/4G) system to [ITU-T](http://en.wikipedia.org/wiki/ITU-T) in late 2009, was approved into ITU, International Telecommunications Union, IMT-Advanced and was finalized by 3GPP in March 2011.[[1]](http://en.wikipedia.org/wiki/LTE_Advanced#cite_note-0) It is standardized by the [3rd Generation Partnership Project](http://en.wikipedia.org/wiki/3rd_Generation_Partnership_Project) (3GPP) as a major enhancement of the [Long Term Evolution](http://en.wikipedia.org/wiki/Long_Term_Evolution) (LTE).standard.

**MAC address (Media Access Control):** Also known as the hardware address or Ethernet address. A unique identifier specific to the network card inside a computer. Allows the DHCP server to confirm that the computer is allowed to access the network. MAC addresses are written as XX-XX-XX-XX-XX-XX, where the Xs represent digits or letters from A to F.

**Mac OS:** is a series of [graphical user interface](http://en.wikipedia.org/wiki/Graphical_user_interface)-based [operating systems](http://en.wikipedia.org/wiki/Operating_system) developed by [Apple Inc.](http://en.wikipedia.org/wiki/Apple_Inc.) (formerly Apple Computer, Inc.) for their [Macintosh](http://en.wikipedia.org/wiki/Macintosh) line of [computer systems](http://en.wikipedia.org/wiki/Computer_system). The Macintosh user experience is credited with popularizing the graphical user interface. The original form of what Apple would later name the "Mac OS" was the integral and unnamed system software first introduced in 1984 with the [original Macintosh](http://en.wikipedia.org/wiki/Macintosh_128K), usually referred to simply as the **System** software.

**Macro virus:** Ultimate presentation of the virus. They are transported in application files (Word, Excel, etc.) and not in binary files (how traditional viruses are). They are executed on the opening of the data file in which they are contained.

**Mainframe computers:** An industry term for a large computer, typically manufactured by a large company such as IBM for the commercial applications and other large-scale computing purposes.

**Malware:** Malicious software. Any programme whose objective is to cause damage to computers, systems or networks and, as a result, to its users.

**Memory cache:** A type of memory that temporarily stores information that is used frequently to enable rapid access to this data.

**Memory cards:** are devices for storing digital information. They are often used in many electronic devices such as digital cameras, mobile phones, laptop computers, music players and games consoles. They are able to retain data without power and come in a variety of capacities, meaning they can store huge amounts of data while being easy to hide from view.

**Memory devices:** A memory device is any device that is capable of storing data either permanently or non-permanently.

**Metadata:** Metadata is information about a combination of files and / or folders that can describe, for example, how and when it was created, received, accessed and modified and by whom. This data is utilised in Computer Forensics to reconstruct the chain of events associated to the analysed file. Depending on the context in which the term is employed, it can refer to one piece of data or another.

**Microprocessors:** incorporates the functions of a [computer](http://en.wikipedia.org/wiki/Computer)'s [central processing unit](http://en.wikipedia.org/wiki/Central_processing_unit) (CPU) on a single [integrated circuit](http://en.wikipedia.org/wiki/Integrated_circuit), (IC) or at most a few integrated circuits. It is a multipurpose, [programmable](http://en.wikipedia.org/wiki/Computer_program) device that accepts [digital data](http://en.wikipedia.org/wiki/Digital) as input, processes it according to instructions stored in its memory, and provides results as output. It is an example of [sequential digital logic](http://en.wikipedia.org/wiki/Sequential_logic), as it has internal memory. Microprocessors operate on numbers and symbols represented in the [binary numeral system](http://en.wikipedia.org/wiki/Binary_numeral_system).

**COFEE: Computer Online Forensic Evidence Extractor** is a tool kit, developed by [Microsoft](http://en.wikipedia.org/wiki/Microsoft), to help [computer forensic investigators](http://en.wikipedia.org/wiki/Computer_forensics) extract evidence from a [Windows](http://en.wikipedia.org/wiki/Windows) [computer](http://en.wikipedia.org/wiki/Personal_computer). Installed on a [USB flash drive](http://en.wikipedia.org/wiki/USB_flash_drive) or other [external disk drive](http://en.wikipedia.org/wiki/External_hard_disk_drive), it acts as an automated forensic tool during a [live analysis](http://en.wikipedia.org/wiki/Computer_forensics#Live_analysis). Microsoft provides COFEE devices and online technical support free to law enforcement agencies.

**Microsoft PubCenter** is a publisher's [ad serving](http://en.wikipedia.org/wiki/Ad_serving) application developed by [Microsoft](http://en.wikipedia.org/wiki/Microsoft) in addition to [Microsoft adCenter](http://en.wikipedia.org/wiki/Microsoft_adCenter), which allows advertisers to place ads on search engines as well as select [MSN](http://en.wikipedia.org/wiki/Microsoft_Network) websites or applications. Currently, in its beta version.

**Microsoft Windows** is a series of [graphical interface](http://en.wikipedia.org/wiki/Graphical_user_interface) [operating systems](http://en.wikipedia.org/wiki/Operating_system) developed, marketed, and sold by [Microsoft](http://en.wikipedia.org/wiki/Microsoft).

**Minicomputers:** is a term for a class of smaller [computers](http://en.wikipedia.org/wiki/Computer) that evolved in the mid-1960s and sold for much less than mainframe and mid-size computers from [IBM](http://en.wikipedia.org/wiki/IBM) and its direct competitors.

**Modem:** MOdulator/DEModulator. A device used by computers to communicate over telephone lines. It is usually recognized by connection to a phone line, but there are also cable modems based on the DSL technology (e.g., cable modems). Can be combined with a facsimile (fax) functionality within a PC card (adapted from).

**Modular rack-mounted systems:** Modular rack-mounted systems are computer systems that are hosted in a rack and often times are built in a modular way allowing each hardware module to be replaced instantly without having negative impacts on the whole system. These racks most usually can host multiple computer systems with 19” form factor.

**Mozilla Firefox** is a [free and open source](http://en.wikipedia.org/wiki/Free_and_open_source_software) [web browser](http://en.wikipedia.org/wiki/Web_browser) developed for [Microsoft Windows](http://en.wikipedia.org/wiki/Microsoft_Windows), [Mac OS X](http://en.wikipedia.org/wiki/Mac_OS_X), and [Linux](http://en.wikipedia.org/wiki/Linux) coordinated by [Mozilla Corporation](http://en.wikipedia.org/wiki/Mozilla_Corporation) and [Mozilla Foundation](http://en.wikipedia.org/wiki/Mozilla_Foundation). Firefox uses the [Gecko](http://en.wikipedia.org/wiki/Gecko_%28layout_engine%29) [layout engine](http://en.wikipedia.org/wiki/Layout_engine) to render web pages, which implements current and anticipated [web standards](http://en.wikipedia.org/wiki/Web_standards).

**Network interface cards:** Provides network connection (either with cable or wireless). Can be in the form of an expansion board or a PC card.

**NTFS** (New Technology File System): is a proprietary [file system](http://en.wikipedia.org/wiki/File_system) developed by [Microsoft Corporation](http://en.wikipedia.org/wiki/Microsoft) for its [Windows](http://en.wikipedia.org/wiki/Microsoft_Windows) line of [operating systems](http://en.wikipedia.org/wiki/Operating_systems), beginning with [Windows NT 3.1](http://en.wikipedia.org/wiki/Windows_NT_3.1) and [Windows 2000](http://en.wikipedia.org/wiki/Windows_2000), including [Windows XP](http://en.wikipedia.org/wiki/Windows_XP), [Windows Server 2003](http://en.wikipedia.org/wiki/Windows_Server_2003), and all their successors to date.

**Online service provider:** can for example be an [internet service provider](http://en.wikipedia.org/wiki/Internet_service_provider), email provider, news provider (press), entertainment provider (music, movies), search, e-shopping site (online stores), e-finance or e-banking site, e-health site, e-government site, [Wikipedia](http://en.wikipedia.org/wiki/Wikipedia), [Usenet](http://en.wikipedia.org/wiki/Usenet). In its original more limited definition it referred only to a commercial computer communication service in which paid members could dial via a computer modem the service's private computer network and access various services and information resources such a [bulletin boards](http://en.wikipedia.org/wiki/Bulletin_board), [downloadable](http://en.wikipedia.org/wiki/Download) [files](http://en.wikipedia.org/wiki/Computer_file) and [programs](http://en.wikipedia.org/wiki/Computer_programs), [news articles](http://en.wikipedia.org/wiki/Newsgroup), [chat rooms](http://en.wikipedia.org/wiki/Chat_room), and [electronic mail](http://en.wikipedia.org/wiki/E-mail) services.

**P2P-Peer to Peer:** Protocol that uses the internet for the interchange and download of files. The term P2P comes from *peer-to-peer* and refers to a network of equals, meaning that the status of each client is the same. The existence of servers in the practical application of the P2P networks is due to the fact that its clients do not possess fixed IP addresses. As a consequence these servers only offer a listing of clients and file searches.

**Pagers:** A pager is a device that may be used for sending and receiving electronic messages, numeric (e.g., phone numbers) and alphanumeric (text, often including e-mail)

**Parallel port dongle:** A small device with a parallel port connector that may provide programmable memory, remote update, lease control algorithms or counters.

**Partitions:** is the act of dividing a [hard disk drive](http://en.wikipedia.org/wiki/Hard_disk_drive) into multiple logical storage units referred to as *partitions*, to treat one physical disk drive as if it were multiple disks. Partitions are also termed "[slices](http://en.wikipedia.org/wiki/Slice_%28disk%29)" for operating systems based on [BSD](http://en.wikipedia.org/wiki/BSD), [Solaris](http://en.wikipedia.org/wiki/Solaris_%28operating_system%29) or [GNU Hurd](http://en.wikipedia.org/wiki/GNU_Hurd). A [partition editor](http://en.wikipedia.org/wiki/Partition_editor) software program can be used to create, resize, delete, and manipulate these partitions on the hard disk.

**Peripheral Devices:** are not an integral part of the computer but connect to it to improve its capabilities. Examples of peripheral devices are: scanners, printers, tape drives, webcams, loudspeakers, microphones, fax , answering machines and card readers.

**Personal Digital Assistant** (PDA): A small (i.e., pocket-sized) device that can include computing, telephone/fax, paging, networking, and other features.

**PGP:** Pretty Good Privacy. Freeware cryptography software (see, e.g., www.pgpI.org) originally developed by Philip R. Zimmermann in 1991. Can be used to encrypt/sign e-mails or encrypt computer files. There is also a low-cost commercial version.

**Pharming:** A technique with the same objective as *Phishing*, but is not based on misleading the user but the Domain Named System (DNS) instead. In this way, if the user’s ISP utilizes vulnerable DNSs, the “pharmer” redirects all the traffic of the URLs that are of interest, to the servers under his/her control. These have an identical appearance to the originals. The only way to detect this type of attack is through the certified servers that, in the case of the “pharmer”, will not have a Certification of Authority.

**Phishing:** Technique of deception that combines social engineering with certain technical tricks with the objective of stealing personal banking information from an individual user. *Phishing* attacks cleverly take the appearance of e-mails from a trusted entity requesting bank details or passwords of the user.

**Phreaker or Phreak:** IT pirate specialised in using telephone networks to access other people’s systems or often just to avoid paying telephone bills. The techniques used by *Phreakers* are commonly known as *phreaks*.

**Programme pirating:** Activity of copying, distributing or using existing IT programmes, infringing legally upon the intellectual property rights that protect its authors.

**POP3:** Post Office Protocol. An Internet service based on a standardized protocol for retrieving e-mail messages from the mail server (i.e., POP server).

**Port replicators:** A device containing common PC ports such as serial, parallel, and network ports that plugs into a portable computer. A port replicator is similar to a docking station, but docking stations normally provide capability for additional expansion boards.

**Portable media players:** store and play digital media such as music and other audio, images, video as well as other files including documents and other types of fields that are capable of being stored digitally.

**Proxy:** In [computer networks](http://en.wikipedia.org/wiki/Computer_network), a **proxy server** is a [server](http://en.wikipedia.org/wiki/Server_%28computing%29) (a computer system or an application) that acts as an intermediary for requests from [clients](http://en.wikipedia.org/wiki/Client_%28computing%29) seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server. The proxy server evaluates the request as a way to simplify and control their complexity. Today, most proxies are **web proxies**, facilitating access to content on the [World Wide Web](http://en.wikipedia.org/wiki/World_Wide_Web).

**Qwerty:** is the most common modern-day [keyboard layout](http://en.wikipedia.org/wiki/Keyboard_layout).

**RAM** **memory:** RAM stands for *Random Access Memory.* RAM memory temporarily stores data that the computer is working with. This memory loses its content as a result of a power loss.

**Recovered data:** The term that identifies recovered or reconstructed files or folders that had been deleted from the active data area. These files can be recovered with the original size and format or in small fragments that will require a forensic reconstruction task.

**Refusal of service:** Incident where a user or an organisation are refused access to a resource they can normally use. Usually, the loss of access is due to the unavailability of a particular network service, such as e-mail, or the temporary loss of all network connections and services. In the worst case, for example, a website where millions of people access can be forced temporarily to cease operating. Although, normally intentional and malicious these type of attacks sometimes occur accidentally. If these attacks do not always result in the theft of information, they almost invariably cost a lot of time and money to the person or organisation affected.

**Reverse engineering:** Consists of the analysis of the binary code of a programme or application to determine its behaviour.

**RIPE Réseaux IP Européens (RIPE,** [French](http://en.wikipedia.org/wiki/French_language) **for "European IP Networks"):** is a forum open to all parties with an interest in the technical development of the [Internet](http://en.wikipedia.org/wiki/Internet). The RIPE community’s objective is to ensure that the administrative and technical coordination necessary to maintain and develop the Internet continues. It is not a standardisation organisation like the [IETF](http://en.wikipedia.org/wiki/Internet_Engineering_Task_Force) and does not deal with [domain names](http://en.wikipedia.org/wiki/Domain_name) like [ICANN](http://en.wikipedia.org/wiki/ICANN).

**Routers:** is a device that determines the next network point that a packet should be forwarded towards its destination. It must be connected to at least 2 networks. It is intelligent and works on routing tables. Although it is located at the gateway to a network it does not necessarily have to be the networks gateway to the Internet.

**Scheduler:** is the method by which [threads](http://en.wikipedia.org/wiki/Thread_%28computer_science%29), [processes](http://en.wikipedia.org/wiki/Process_%28computing%29) or data [flows](http://en.wikipedia.org/wiki/Flow_%28computer_networking%29) are given access to system resources (e.g. processor time, communications bandwidth). This is usually done to [load balance](http://en.wikipedia.org/wiki/Load_balancing_%28computing%29) a system effectively or achieve a target [quality of service](http://en.wikipedia.org/wiki/Quality_of_service). The need for a scheduling algorithm arises from the requirement for most modern systems to perform [multitasking](http://en.wikipedia.org/wiki/Computer_multitasking) (execute more than one process at a time) and [multiplexing](http://en.wikipedia.org/wiki/Multiplexing) (transmit multiple flows simultaneously).

**SHA-256 hash:** is a set of [cryptographic hash functions](http://en.wikipedia.org/wiki/Cryptographic_hash_function) (**SHA-224, SHA-256, SHA-384, SHA-512**) designed by the [National Security Agency](http://en.wikipedia.org/wiki/National_Security_Agency) (NSA) and published in 2001 by the [NIST](http://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology) as a U.S. [Federal Information Processing Standard](http://en.wikipedia.org/wiki/Federal_Information_Processing_Standard). SHA stands for [Secure Hash Algorithm](http://en.wikipedia.org/wiki/Secure_Hash_Algorithm). SHA-2 includes a significant number of changes from its predecessor, [SHA-1](http://en.wikipedia.org/wiki/SHA-1). SHA-2 consists of a set of four hash functions with digests that are 224, 256, 384 or 512 bits.

**Slack area data:** Due to the necessity of the computer to assign fixed sized blocks of disk space, there exists an area at the end of every file that, despite being assigned to the file, contains information not relating to the other information contained therein. This area is called “slack” and contains information of the contents that were on this block space before it was assigned a new file.

**Slack space:** Slack space is an area of space on a storage devices that is allocated to a certain unit, e.g. a file, a partition, a disk, an MFT record but is not used by this unit. Oftentimes a forensic specialist can find data belonging to formerly stored files in these slack spaces. If for example a cluster gets allocated to a newly created file but the data of this file do not use the whole cluster than there is a good chance to find traces of a previously stored file in the slack space of the cluster.

**Social Engineering:** Techniques or skills that allow manipulation of a person that, voluntarily carries out actions that they normally would not do, such as the revealing of information.

**Software:** Computer programs designed to perform specific tasks, such as word processing, accounting, network management, Website development, file management, or inventory management.

**Solid state disks:** they store information in a different way than hard disks, while intending to provide access in the same way as tradtional hard disks. Whereas hard disks store data on platters, solid state disks store data using microchips that have no moving parts. As such they are less likely to be damaged by shock and they offer faster access to the data. These devices may hold valuable evidence.

**Speaker magnets:** Common speakers consist of a magnet, a coil and a cone. The speaker magnet is there to provide a permanent magnetic field for the the speaker coil, which is embedded in the paper of the speaker cone. When the audio signal flows throw the speaker coil it generates a small magnetic field the strength of which varies with the strength of the audio signal. This small magnetic field is repelled by or attracted to the permanent magnetic field produced by the speaker magnet.

**Storage devices:** is a device for [recording](http://en.wikipedia.org/wiki/Recording) (storing) [information](http://en.wikipedia.org/wiki/Information) (data). Recording can be done using virtually any form of [energy](http://en.wikipedia.org/wiki/Energy), spanning from manual muscle power in [handwriting](http://en.wikipedia.org/wiki/Handwriting), to acoustic vibrations in [phonographic](http://en.wikipedia.org/wiki/Phonograph) recording, to electromagnetic energy modulating [magnetic tape](http://en.wikipedia.org/wiki/Magnetic_tape) and [optical discs](http://en.wikipedia.org/wiki/Optical_disc).

**Tablet Devices:** A tablet computer is a device that is operated by touching the screen rather than using a keyboard or mouse. It is normally larger than a mobile phone or **Personal Digital Assistant**

**Traceable:** Traceability refers to the completeness of the information about every step in a [process chain](http://en.wikipedia.org/w/index.php?title=Process_chain&action=edit&redlink=1). The formal definition of traceability is the ability to chronologically interrelate uniquely identifiable entities in a way that is verifiable. Traceability is the ability to verify the history, location, or application of an item by means of documented recorded identification.

**TrueCrypt:** is a free [software application](http://en.wikipedia.org/wiki/Software_application) used for [on-the-fly encryption](http://en.wikipedia.org/wiki/On-the-fly_encryption) (OTFE). It can create a virtual encrypted disk within a file or encrypt a [partition](http://en.wikipedia.org/wiki/Disk_partitioning) or (under [Microsoft Windows](http://en.wikipedia.org/wiki/Microsoft_Windows) except [Windows 2000](http://en.wikipedia.org/wiki/Windows_2000)) the entire [storage device](http://en.wikipedia.org/wiki/Data_storage_device) ([pre-boot authentication](http://en.wikipedia.org/wiki/Pre-boot_authentication)).

**Trusted Platform Module (TPM):** Most commonly the concept of TPM is applied in a TPM cryptoprocessor, known as TPM chip. This chip which is responsible for carrying out the TPM tasks is soldered to the mainboard of a computer system. The primary scope of a TPM is to assure the integrity of a platform. In this context "integrity" means "behave as intended" and a "platform" is generically any computer platform: Start the power-on boot process from a trusted condition and extend this trust until the OS has fully booted and applications running. TPM is also oftentimes used in combination with disk encryption, e.g. Truecrypt or Bitlocker Full Disk Encryption where it is used to protect the keys used to encrypt the computer's hard disks and provide integrity authentification for a trusted boot pathway.

**Ubuntu Linux:** is a computer [operating system](http://en.wikipedia.org/wiki/Operating_system) based on the [Debian](http://en.wikipedia.org/wiki/Debian) [Linux distribution](http://en.wikipedia.org/wiki/Linux_distribution) and distributed as [free and open source software](http://en.wikipedia.org/wiki/Free_and_open_source_software), using its own [desktop environment](http://en.wikipedia.org/wiki/Desktop_environment). It is named after the [Southern African](http://en.wikipedia.org/wiki/Southern_Africa) philosophy of [ubuntu](http://en.wikipedia.org/wiki/Ubuntu_%28philosophy%29) ("humanity towards others"). Ubuntu is designed primarily for use on [personal computers](http://en.wikipedia.org/wiki/Personal_computer), although a [server](http://en.wikipedia.org/wiki/Server_%28computing%29) edition also exists.

**Universal Serial Bus (USB):** is a standard that defines the protocols for communication, connection and power supply for devices that are to be connected to computers. Since its advent in the 1990s the number of devices that are now capable of being connected using this protocol has grown and new devices in all sorts of shapes and sizes are now used to store data.

**Unix:** is a [multitasking](http://en.wikipedia.org/wiki/Computer_multitasking), [multi-user](http://en.wikipedia.org/wiki/Multi-user) computer [operating system](http://en.wikipedia.org/wiki/Operating_system) originally developed in 1969.

**Untrusted binaries:** The term “untrusted binary” is most often used in conjunction with executable binary files that are stored or copied from an untrusted source. Any source that cannot be verified or has not undergone defined close validation procedures may potentially contain altered or even harmful source code and therefore should be considered untrusted. A typical example for untrusted binaries are executable files that are stored on a system other that the validated machine of the forensic specialist.

**Unused or unassigned area data:** Data that presently resides in the disk area that does not belong to a file; the remainder of the deleted digital documents.

**URL(Uniform Resource Locator):** A chain of characters which is assigned a unique address to each of the documents of the World Wide Web (*news, gopher*, etc.)

**UTorrent:** is a [freeware](http://en.wikipedia.org/wiki/Freeware), [closed source](http://en.wikipedia.org/wiki/Closed_source) [BitTorrent client](http://en.wikipedia.org/wiki/BitTorrent_client) now owned by [BitTorrent, Inc](http://en.wikipedia.org/wiki/BitTorrent_%28company%29). It is the most widely used BitTorrent client outside China (where [Xunlei](http://en.wikipedia.org/wiki/Xunlei) is more popular). It gets the "[µ](http://en.wikipedia.org/wiki/%CE%9C)" in its name from the [SI prefix](http://en.wikipedia.org/wiki/SI_prefix) "[micro-](http://en.wikipedia.org/wiki/Micro-)", referring to the program's small [memory footprint](http://en.wikipedia.org/wiki/Memory_footprint): the program was designed to use minimal computer resources while offering functionality comparable to larger BitTorrent clients such as [Vuze](http://en.wikipedia.org/wiki/Vuze) or [BitComet](http://en.wikipedia.org/wiki/BitComet). The program has received consistently good reviews for its feature set, performance, stability, and support for older hardware and versions of Windows.

**Virtual environment:** The computational simulation of a work environment formed by the interconnection of multiple computers that permits the access to digital information independent of their physical location.

**Virus:** Programme that can infect other programmes, modifying them to include a copy of itself. Viruses basically have the function of propagation and replication but, furthermore, there are some that have harmful contents (*payload*) with different objectives, from a simple joke to causing serious damage to systems. These types of programmes can operate in various ways: Only notifying the user of its presence without causing apparent damage, Attempt to go unnoticed to cause the most damage possible or Take possession of the principal functions (to infect the filing system).

**VoIP:** Voice over Internet Protocol. The technology used to transmit voice conversations over a data network using the Internet protocol. Data network may be the Internet or a corporate Internet.

**Volatile Data:**Volatile Data are data that are digitally stored in a way that the probability is very high for their contents to get deleted, overwritten or altered in a short amount of time by human or automated interaction.

**Warez:** Pirate copies of programmes. Protected software versions that have had the protection removed.

**Web Browser:** A web browser can also be defined as an [application software](http://en.wikipedia.org/wiki/Application_software) or program designed to enable users to access, retrieve and view documents and other resources on the [Internet](http://en.wikipedia.org/wiki/Internet).

**Windows Explorer:** is a [file manager](http://en.wikipedia.org/wiki/File_manager) application that is included with releases of the [Microsoft Windows](http://en.wikipedia.org/wiki/Microsoft_Windows) [operating system](http://en.wikipedia.org/wiki/Operating_system) from [Windows 95](http://en.wikipedia.org/wiki/Windows_95) onwards. It provides a [graphical user interface](http://en.wikipedia.org/wiki/Graphical_user_interface) for accessing the [file systems](http://en.wikipedia.org/wiki/File_system). It is also the component of the operating system that presents many user interface items on the [monitor](http://en.wikipedia.org/wiki/Computer_display) such as the [taskbar](http://en.wikipedia.org/wiki/Taskbar) and [desktop](http://en.wikipedia.org/wiki/Desktop_environment). Controlling the computer is possible without Windows Explorer running (for example, the File | Run command in Task Manager on NT-derived versions of Windows will function without it, as will commands typed in a command prompt window).

**Wireless Modems:** A wireless modem is a type of modulator-demodulator which connects to a wireless network instead of using telephone or cable television lines. A mobile Internet user can connect using a wireless modem to a wireless Internet Service Provider (ISP) to get Internet access.

**WireShark:** is a [free and open-source](http://en.wikipedia.org/wiki/Free_and_open_source_software) [packet analyser](http://en.wikipedia.org/wiki/Packet_analyzer). It is used for [network](http://en.wikipedia.org/wiki/Computer_network) troubleshooting, analysis, software and [communications protocol](http://en.wikipedia.org/wiki/Communications_protocol) development, and education. Originally named **Ethereal**, in May 2006 the project was renamed Wireshark due to trademark issues.

**WLAN networks:** wireless local area network (WLAN) links two or more devices using some wireless distribution method (typically [spread-spectrum](http://en.wikipedia.org/wiki/Spread_spectrum) or [OFDM](http://en.wikipedia.org/wiki/OFDM) radio), and usually providing a connection through an access point to the wider internet. This gives users the mobility to move around within a local coverage area and still be connected to the network. Most modern WLANs are based on [IEEE 802.11](http://en.wikipedia.org/wiki/IEEE_802.11) standards, marketed under the [Wi-Fi](http://en.wikipedia.org/wiki/Wi-Fi) brand name.

**Word Processor:** A software program used to turn the computer into a typewriter for wiring letters, reports and documents. Common Word Processing programs: Wordstar, Wordperfect, MS-Word.

**Worm:** IT programme that auto-duplicates and auto-propagates. In contrast with viruses, worms are usually written especially for networks. Network worms were first defined by Shoch & Hupp, of Xerox, in the magazine *ACM Communications* (March 1982). The first famous internet worm appeared in November 1988 propagated itself to more than 6,000 systems at large on the internet.

**WWW (World Wide Web):** The universe of network-accessible information, i.e., all the resources and users on the Internet that are using the Hypertext Transfer Protocol (HTTP)

**ZIP drives:** A removable hard disk system. A ZIP drive is a small, portable disk drive used primarily for backing up and archiving personal computer files. The trademarked ZIP drive was developed and is sold by Iomega Corporation. Zip drives and disks come in two sizes.

1. The Council of Europe Convention on Cybercrime (ETS No.185) [↑](#footnote-ref-1)
2. Image Source:

   [1] computershopper.com/var/ezwebin\_site/storage/images/desktops/product-profile/ superior -699-pc-model-6173/38202-1-eng-US/superior-699-pc-model-61731\_product\_review\_ thumb.jpg

   [2] expresscomputing.info/siteimages/laptop1.jpg

   [3] prepare.icttrends.com/images/2012/06/mainframe-computer.jpg [↑](#footnote-ref-2)
3. Image Source

   [8] upload.wikimedia.org/wikipedia/commons/e/e6/Hard\_disk\_Western\_Digital\_WD1000\_1\_ (dark1).jpg

   [9] lh3.ggpht.com/\_Kkg7XHt7mJA/TLHZioMTiBI/AAAAAAAAAow/FN4THl-QzNQ/s800/Storage-Hard-disk.jpg

   [10] blog.mirchimart.com/wp-content/uploads/2012/06/1.jpg [↑](#footnote-ref-3)
4. Also called Digital Versatile Disk [↑](#footnote-ref-4)
5. Image Source:

   [11] jetmedia.co.uk/cdmada80.jpg

   [12] 3.bp.blogspot.com/\_RzAQQvY1zGw/TPHH3KzB3rI/AAAAAAAAAWg/ctwmTTfTgew/s1600/icon-DVD.png

   [13] 4.bp.blogspot.com/\_N3kyjbXGs0I/S3OK\_6rfzLI/AAAAAAAAADY/S76APQ9wVPE/s320/sony-blu-ray-disc-format-us.jpg [↑](#footnote-ref-5)
6. Image Source

   [14] memorycardsforcameras.org/wp-content/uploads/memory-cards-for-cameras-sd.sdhc\_ .sdxc\_.jpg

   [15] portal.lynxmobility.com/images/Accesssories/microSD\_2GB\_02.jpg

   [16] heise.de/imgs/18/4/8/6/8/6/8/SP128GBCFC400V10.jpg-777a6b1cc6a3f2fc.jpeg [↑](#footnote-ref-6)
7. Image Source

   [17] img.ehowcdn.com/article-new/ehow/images/a07/ph/ee/clean-usb-ports-laptop-computers-800x800.jpg

   [18] s0.static.mymemory.co.uk/images/product\_shots/large\_16631\_1297420753.jpg

   [19] 1.bp.blogspot.com/\_o801UUtSFEI/TPuVqLOz3qI/AAAAAAAAACM/-XvKYezjX-E/s1600/ 2edsfas.jpg

   [20] merchandisemania.co.uk/productimages/fullsize/XH21-Metal--USB-Flash-Drive-With-Clear-Ends-STR-CAP-OFF/Personalised-Printed--Metal--USB-Flash-Drive-With-Clear-Ends.jpg

   [21] media.tecca.com/2010/11/03/630-usb-lexar-630w.jpg

   [22] 1.pcmag.com/media/images/310963-verbatim-tuff-n-tiny-usb-drive.jpg?thumb=y

   [23] 3.bp.blogspot.com/\_zS2JDRBdNzk/THd83p8BZ8I/AAAAAAAACKc/sgBaS8XLbbg/s1600/4mm +pico-usb-300x261.jpg [↑](#footnote-ref-7)
8. Image Source:

   [24] ohgizmo.com/images/imation\_4gb\_micro\_hard\_drive.jpg

   [25] media.gdgt.com/img/product/11/8ov/oakley-thump-i3m-800.jpg

   [26] technabob.com/blog/wp-content/uploads/2006/09/imation\_usb\_wristbands.jpg

   [27] pixelbeat.org/systems/laks/usb-watch-drive-uf1s.jpg

   [28] cookingfor.us/catalog/images/Victorinox%20SwissMemory%20128%20MB% 20USB%20Storage.jpg

   [29] geeky-gadgets.com/wp-content/uploads/2008/01/domino\_thumb\_drive.jpg [↑](#footnote-ref-8)
9. "open-format" means that users have access to multiple compatible sources of storage media. Source: http://searchstorage.techtarget.com/definition/Linear-Tape-Open [↑](#footnote-ref-9)
10. Image Source

    [30] 2.imimg.com/data2/LO/TG/MY-3658176/fujifilm-linear-tape-open-lto5-250x250.jpg

    [31] global.tdk.com/csr/ecolove/img/eco\_med03.jpg

    [32] 3000newswire.blogs.com/.a/6a00d83452e85869e20134809149c4970c-320wi [↑](#footnote-ref-10)
11. Image Source:

    [33] softwaretutor.files.wordpress.com/2010/04/fax.jpg

    [34] superwarehouse.com/images/products/hpQ3851AA2L.jpg

    [35] static.bhphoto.com/images/images345x345/504534.jpg

    [36] carolinabarcode.com/images/ArticleImages/RunMyStore/CreditCardReader.jpg

    [37] xactcommunication.com/itempics/48\_xlarge.jpg

    [38] labelprinter.org.uk/wp-content/uploads/2009/03/dymo-labelwriter-400.jpg [↑](#footnote-ref-11)
12. A kind of wireless 4G broadband network. [↑](#footnote-ref-12)
13. Image Source:

    [4] find-cool.net/wp-content/uploads/2012/09/Windows-8-Tablet-PC.jpg

    [5] vedainformatics.com/blogs/wp-content/uploads/2010/01/apple-ipad-tablet-pc.png

    [6] comparetablets.co.uk/wp-content/uploads/2011/09/galaxy-tab-8.9.jpg

    [7] cache.gizmodo.com/assets/images/4/2007/12/delltablet.jpg [↑](#footnote-ref-13)
14. Image Source:

    [39] lh5.googleusercontent.com/-RyY55\_39t7o/T25v61iDZnI/AAAAAAAAADc/fW-gqm7QTR4/s0 /phone.png

    [40] resources.envirofone.com/shared/media/images/news/articles/mobile\_phone\_recycling\_could \_ be \_boosted\_by\_iphone\_4\_deals\_2059\_19917932\_0\_0\_7063723\_300.jpg

    [41] fonesunlock*.co.uk/images/P/Unlock\_Blackberry\_Storm\_9500-01.jpg* [↑](#footnote-ref-14)
15. For instance, using the Exchangeable Image Format (EXIF) standard. [↑](#footnote-ref-15)
16. Image Source

    [42] transcribe.co.uk/UserFiles/digital\_camera\_picture(3).jpg

    [43] brain.pan.e-merchant.com/6/0/12305806/l\_12305806.jpg

    [44] cdn0.mos.techradar.futurecdn.net///classifications/gadgets/digital-cameras/images/ canoneos1dmarkiiiangled-380-75.jpg

    [45] bridgetoworld.com/images/l/201009/12834167310.jpg

    [46] cdn2.bigcommerce.com/server1700/0a80b/products/60/images/291/Digital\_spy\_alarm\_ clock\_3\_\_74576.1282420400.1280.1280.gif

    [47] wholesales-shopping.com/wp-content/uploads/2011/09/17.jpg

    [48] images.madeinchina.com/p/520/3593520\_0/On-sale-4GB-Spy-Camera-Watch-Video-Recorder-Mini\_3593520\_0.bak.jpg [↑](#footnote-ref-16)
17. Image Source:

    [49] alpha.akihabaranews.com/wp-content/uploads/images/6/66/16666//1.jpg

    [50] sils.unc.edu/sites/default/files/it/CanonGL2.jpg

    [51] pembrokeshirefilmfestival.files.wordpress.com/2012/12/panasonic-hcv100.png [↑](#footnote-ref-17)
18. Image Source

    [52] blogcdn.com/www.switched.com/media/2008/07/41113\_4048.jpg

    [53] totalsecuritywarehouse.com/images/catalog/category50.jpg [↑](#footnote-ref-18)
19. Image source

    [54] i.ebayimg.com/t/8GB-Digital-Voice-Recorder-650Hr-Dictaphone-MP3-Player-w-U-Disk-Iron-gray-US-/00/s/MTAwMFgxMDAw/$(KGrHqNHJEgFDTE6vHM3BQ7nlu,LGg~~60\_35.JPG

    [55] c773974.r74.cf2.rackcdn.com/0330731\_617464.jpg

    [56] fl12.shopmania.org/files/p/bg/t/472/m-audio-micro-track-ii~3964472.jpg [↑](#footnote-ref-19)
20. Image Source

    [57] newlonsoft.com/images/CCTV%20images/CCTV-Camera\_2.jpg

    [58] videos.cctvcamerapros.com/images/ptz-cameras/infrared-ptz-camera.jpg

    [59] icode.co.uk/icatcher/cctvshop//images/Genie-VRD43-Dome-CCTV-Camera.jpg

    [60] goldlinesecuritysystems.com/wp-content/uploads/2011/07/balajicctv\_gif.jpg [↑](#footnote-ref-20)
21. ‘Moving Picture Expert Group Audio Layer‘3 [↑](#footnote-ref-21)
22. *Image source:*

    *[61] newsongs2013.net/mp3-player-2010-images/best-mp3-player-2010-apple-ipod-touch.jpg*

    *[62] butzgaskins.com/wp-content/uploads/2012/04/iPods-MP3-Players1.jpg*

    *[63] geekalerts.com/u/cross-mp3-player.jpg*

    *[64] images.highspeedbackbone.net/skuimages/large/Creative-Labs-Zen-Stone-1Mai.jpg*

    *[65] ecodigital.co.uk/estore/images/sandisk-sansa-fuze.jpg* [↑](#footnote-ref-22)
23. *Image Source  
    [66] static1.thcdn.com/productimg/0/600/600/41/10179241-1279698066-442000.jpg*

    *[67] gadgetsin.com/uploads/2011/01/sony\_psp\_2\_codenamed\_ngp\_1.jpg*

    *[68] galaxine.com/gifs/console.jpg*

    *[69] ecx.images-amazon.com/images/I/41XM4A0DD6L.\_SL500\_AA300\_.jpg*

    *[70] game-consoles.org/wp-content/uploads/2010/11/nintendo-3ds-video-game-console.jpg*

    *[71] venturebeat.files.wordpress.com/2012/07/ouya-big.jpg?w=558&h=9999&crop=0* [↑](#footnote-ref-23)
24. A router is a device that directs or ‘routes’ packets of data along a network or between networks. [↑](#footnote-ref-24)
25. *Image Source*

    *[72] mpcomp.co.uk/5/graphics/import/105481.jpg*

    *[73] resexcellence.com/wp-content/uploads/2013/01/5big\_NAS\_Pro\_back\_34\_left.jpg*

    *[74] gadgetreview.com/wp-content/uploads/2011/03/D-Link-DNS-321-Network-Attached-Storage-Enclosure.jpg* [↑](#footnote-ref-25)
26. *Image source:*

    *[75] ssos.com/nic.jpg*

    *[76] ecx.images-amazon.com/images/I/41CAHWZY8LL.\_SL500\_SS500\_.jpg*

    *[77] hexcs.com/assets/Uploads/TL-WN851N.jpg* [↑](#footnote-ref-26)
27. Image Source

    [78] omnisecu.com/images/basic-networking/network-ethernet-hub.jpg [↑](#footnote-ref-27)
28. *Image source*

    *[79] upload.wikimedia.org/wikipedia/commons/thumb/5/5f/Linksys48portswitch.jpg/220px-Linksys48portswitch.jpg* [↑](#footnote-ref-28)
29. Image Source:

    [80] trendnet.com/image/products/photo/TW100-BRV204\_d3\_2.jpg [↑](#footnote-ref-29)
30. Image Source:

    [81] x3me.info/wp-content/uploads/2011/10/server.jpg

    [82] chost.pl/templates/whm/images/servers.png

    [83] electroguardpaint.com/images/computerServerRoom.jpg [↑](#footnote-ref-30)
31. *Image Source*

    *[84]hacker10.com/wp-content/uploads/2011/04/Hardware-firewall-WatchGuard-XTM-2Series.jpg*

    *[85] plug.4aero.com/Members/lmarzke/talks/plug\_utm/screenshot1.png/image\_preview*

    *[86] cloverline-guardline.com/images/firewall.jpg* [↑](#footnote-ref-31)
32. *Image Source :*

    *[87] solwise.co.uk/images/imageswifi/net-el-ecb3500-1.jpg*

    *[88] zdtronic.com/images/WNDAP330.jpg*

    *[89] amlabels.co.uk/files/images/products/5397.jpg* [↑](#footnote-ref-32)
33. Source: Wikipedia.org [↑](#footnote-ref-33)