

Glossary of Terms

<u>Term</u>	<u>Meaning</u>
ADS	<u>Alternate Data Stream</u> – data stored in the same file as the main data stream but not accessible by default.
Adware	See <i>Malware</i>
APIPA	<u>Automatic Private IP Address</u> – an APIPA address is used by a computer or network device when it has been unable to obtain an IP address from a DHCP server. APIPA address often begin with 169.
Application	See <i>software</i> .
AUP	<u>Acceptable Use Policy</u> – a list of rules that an organisation provides to ensure users are aware of what they may and may not use computer systems for.
BIOS	<u>Basic Input/Output System</u> – the BIOS starts the computer and boots the operating system (OS).
CCTV	<u>Closed Circuit Television</u> – a method used to gather visual surveillance.
CLI	See “Command Prompt”
Command prompt	A command line interface (CLI) where the user enters commands by typing them on the keyboard. Command prompts have little use for a mouse.
Cookie	A text file placed on a system by a website to allow settings to be saved for future visits.
CPU	<u>Central Processing Unit</u> – put simply, the brain of a computer.
Credentials	Generally a pair consisting of <i>username</i> and <i>password</i> .
DACL	<u>Discretionary Access Control List</u> – a list that dictates what users can do to a file or resource. For example, a user might be able to read a file but not modify it. If a user isn't mentioned in the DACL (or referenced to by group membership) then the user cannot access the file or resource.
DC	<u>Domain Controller</u> – Domain Controllers authenticate users to a domain, allowing them to logon and work within defined security perimeter.
DFS	<u>Distributed File System</u> – DFS allows administrators to store files in multiple locations, allowing them to be replicated to more than one place. DFS can also load balance meaning if a large number of users request the same file a single server isn't swamped with requests.
DHCP	<u>Dynamic Host Configuration Protocol</u> automatically configures network cards with an IP address and other administrator configured information (for example gateways, DNS servers).
DLL	<u>Dynamic Link Library</u> – a file on Microsoft Windows that contains code other applications link to to perform a common tasks. Use of DLLs means that functionality can be shared between applications.
DNS	<u>Domain Name System</u> – as humans are better at remembering names than numbers, DNS allows a name to be given to an IP address. For example, www.google.com is an example of DNS which actually translates to 216.239.59.103.
Domain	A Windows Domain is a security boundary that is bound by a set of administrator defined rules. Access to the domain is controlled via Domain Controllers (Dcs) that authenticate users and devices to ensure the boundary is maintained.
Domain Controller	See <i>DC</i> .
DOS	<u>Disk Operating System</u> – DOS was a precursor to the modern OS.
EFS	<u>Encrypting File System</u> – EFS is a feature in Microsoft Windows that allows users to encrypt their files. EFS in the enterprise can be especially useful for protecting corporate data and can also be recovered by administrators with the master key.
Encrypted	See “encryption”.
Encryption	Encryption is a method for taking data and making it unreadable unless the reader knows the password or encryption key used. Various encryption keys exist and generally once a file is encrypted it looks like random junk has been placed in the file.
FAT	<u>File Allocation Table</u> – the filesystem created by Microsoft and the predecessor to <i>NTFS</i> . FAT 32 was unable to handle files larger than 4GB and didn't support setting permissions on files (<i>DACL</i>). FAT is still used on floppy disks and many USB mass storage devices.
FAT12	See <i>FAT</i> .
FAT16	See <i>FAT</i> .
FAT32	See <i>FAT</i> .

Glossary of Terms

Firewall	Software that controls access to the network by permitting or denying incoming and outgoing network traffic. Often firewalls limit traffic based on <i>port</i> or <i>IP Address</i> .
FTP	<u>F</u> ile <u>T</u> ransfer <u>P</u> rotocol – a method for transferring files over a network. FTP sends all usernames, passwords and files in the clear (i.e. not encrypted).
Gateway	Provides connectivity to the Internet, often provided by a router.
GPO	<u>G</u> roup <u>P</u> olicy <u>O</u> bject – a GPO is a set of rules on a Windows system that determines what a user can do. GPOs can define information like what the user sees on their desktop or what options are available to the user in Windows Explorer. GPOs are stored on Domain Controllers (DC) and are regularly updated on client machines.
GUI	<u>G</u> raphical <u>U</u> ser <u>I</u> nterface – unlike the <i>CLI</i> , a GUI is often a mouse driven interface allowing users to see icons and programs in a friendly way. Instead of entering commands by typing, commands are often performed in a GUI by use of a mouse or other pointing device.
Hardware	The physical components of a computer – the bits you can touch. Examples include keyboard, mouse, scanners, printers etc.
Hashing	A process used to generate a numerically defining string for a file. Often used to compare if 2 files are the same (files that are the same will produce the same hash, files that are different won't).
History	A Computer log of activity. Examples include “Internet History” for websites that have been visited and “Command history” for instructions that have been performed.
Honeypot	A honeypot is a system setup specifically to trap malware and viruses (or similar).
Image	While Image can refer to a picture it can also refer to a copy of a computer's hard disk. Disk images can be used for restoring a computer to a previous state but also to preserve the data on the original hard disk if analysis needs to be performed on its data. By taking an image and analysing the contents of the image, analysts can work on a copy of the data, avoiding contamination of the source.
IP Address	<u>I</u> nternet <u>P</u> rotocol <u>A</u> ddress – networked devices need IP addresses to communicate. An example of an IP Address is 192.168.0.3
Kerberos	An authentication mechanism. Kerberos is used by Windows <i>Domain Controllers</i> .
Laptop	A small, portable, workstation consisting of the disk drives, screen, mouse and other components typically found in a static workstation.
Linux	A free operating system (OS) created by Linux Torvalds.
Log	Like a diary, a log contains details of events that occurred with dates and times associated to them. Often a log will show additional information such as the user that performed the action or any relevant error messages.
Log in / Log on	Begin to use a system as a certain person. When logging on users specify a username and password and are then granted access to files and resources.
Log off	To end a user's session, closing any applications they had running.
Malware	Software that an attacker creates with the intention of infiltrating a system and gathering information (steal confidential information (user credentials, bank details) . Malware may, however, just inconvenience the user by causing system problems although this is not normally the malware's sole task.
MBR	<u>M</u> aster <u>B</u> oot <u>R</u> ecord
MFT	<u>M</u> aster <u>F</u> ile <u>T</u> able
Netbook	A more portable form of a <i>laptop</i> , often lacking disk drives and other bulky features.
Non-volatile memory	Memory that is preserved on power off, e.g. files on a hard disk.
Notebook	See <i>laptop</i> .
NTFS	NTFS is filesystem and the successor to <i>FAT</i> . NTFS allows for files larger than 4GB and also can be secured using file permissions (<i>DAcls</i>).
OS	<u>O</u> perating <u>S</u> ystem – the OS allows the user to interact with the hardware of the computer. Without the OS the user would be unable to run any software or perform any tasks.
Partition	An area of disk space.
Password	A word, phrase or string of characters that should only be known to an individual. Along with a <i>username</i> , a password identifies a person to the computer system.
Patch Tuesday	On the first Tuesday of every month Microsoft issues software patches and updates for its software. These can be security fixes, feature improvements and bug corrections and each update is ranked in terms of severity.

Glossary of Terms

PBR	<u>Partition Boot Record</u>
Peripherals	Additional components of a computer system that aren't essential. These include the keyboard and mouse (the computer will function without a keyboard and mouse although will have only limited use to a human).
Port	Like a doorway to a computer. Attackers can only infiltrate a computer if there is software listening on an open port.
Process	When <i>software</i> is running a process is started. Processes have unique IDs that allow the system to allocate resources for use.
Program	See <i>software</i> .
Reboot	Like a <i>shutdown</i> but the computer switches on immediately after it has turned off to allow a user to start again.
Recycle Bin	On Microsoft Windows systems, when a file is deleted it is first moved to the Recycle Bin. Files here can be easily recovered in the event of accidental deletion
Registry	The Windows Registry is a database of settings that control the OS and certain application behaviours. Software often leaves traces in the registry and the registry can be used to start software on logon or startup (amongst others).
SAT	<u>Security Access Token</u> – the SAT contains details of the users SID and group memberships. Windows systems then use the SAT to check if a user is mentioned in a DACL. A new SAT is obtained each time a user logs on to the domain.
Serial number	A string of characters that identifies a particular device (only useful with the manufacturer's name as manufacturers may have the same serial numbering system).
Server	A computer that provides services to another computer. For example, a file server stores files for retrieval by other computers. A <i>DNS</i> server translates <i>IP addresses</i> to names and vice versa.
Service	An application that runs in the background without user interaction.
Shutdown	Safely instructing a computer to switch off causing some temporary files to be flushed and ending all running programs.
SID	<u>Security Identifier</u> – a specific string of characters that uniquely defines a user or device. On a Windows domain, SIDs are used in DACLs to specify permissions.
Slack space	Unallocated disk space, see slide 536-4-20.
SME	<u>Subject Matter Expert</u>
Software	Programs or applications that run on a computer are examples of software. Software cannot be touched and exists digitally only (it is useful to note that the media the software was supplied on is hardware). The Operating System (see OS) is an example of <i>system software</i> .
Spyware	See <i>Malware</i>
SSH	<u>Secure Shell</u> – a secure command line interface that allows users to remotely logon to a server and perform tasks securely.
Steganography	The art of hiding something in plain sight (e.g. invisible ink, writing white text on a white background).
Telnet	Telnet is a method for users to connect to machine and execute commands using a CLI. As telnet sends all usernames, passwords and commands in the clear (i.e. not encrypted) it isn't recommended and SSH should be considered as a replacement.
Trojan	A trojan, or trojan horse, is an item of <i>malware</i> that infiltrates a system by pretending to be something else. For example, trojans may gain access to a system by users downloading a “free screensaver” only to find the computer is now accessible to an attacker.
Truecrypt	A free, open source encryption program capable of encrypting whole disks or creating an encrypted file container where other files can be stored. See www.truecrypt.org for more details.
Uptime	The length of time a system has been switched on and running.
USB	<u>Universal Serial Bus</u> – a method of connecting devices to a computer, often used for printers, keyboards and mice and for mass storage devices (portable hard disks, memory sticks etc).
Username	An account that provides access to the system is identified by a username. Along with a <i>password</i> , a username identifies a person to the computer system.
Virus	A computer program that replicates itself, potentially damaging data causing problems to the user. See also <i>malware</i> .

Glossary of Terms

Volatile evidence	Evidence that is lost on power off, often stored in RAM. Examples include lists of processes running at the time, users that are logged on etc.
Volatile memory	Memory that is lost on power off, e.g. <i>RAM</i> .
Windows	An Operating System (OS) by Microsoft.
Workstation	A client computer (i.e. not a <i>server</i>).