SWINBURNE UNIVERSITY OF TECHNOLOGY

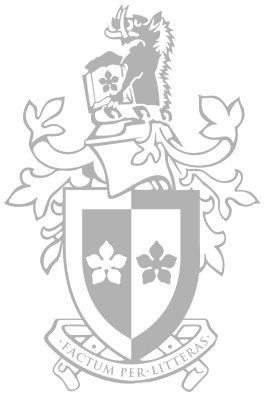
ICT30010 eForensic Fundamentals

Lecture 2

PC Architecture and Operating Systems

Troy PRETTY

Digital Forensic Analyst



SWINBURNE UNIVERSITY OF TECHNOLOGY

Outline and Learning Goals

- Number systems
  - Binary, octal, decimal, hex
- Units of Measurement
- Character sets
  - ASCII and Unicode
- PC architecture
  - Internal components, ports and peripherals
- Operating Systems
  - Windows, Linux and MacOS (OSX)

Binary

- Base 2
- Digits are 0 and 1

Octal

- Base 8
- Digits are 0, 1, 2, 3, 4, 5, 6, 7

Decimal

- Base 10
- Digits are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9

Hexadecimal

- Base 16
- Digits are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F

Number Systems

- Important to know how to distinguish various number systems
- Possible to convert between the various number systems
- Tools to assist with conversion
  - Tables
  - Calculator

Units of Measurement

- Bit (b)
  - Binary digit, 0 or 1
  - Smallest Unit of storage
- Bytes (B)
  - 8 bits
- Kilobyte (KB)
  - 1024 bytes
- Megabyte (MB)
  - 1024 Kilobytes
- Gigabyte (GB)
  - 1024 Megabytes
- Terabyte (TB)
  - 1024 Gigabytes
- Others
  - Nibble, WORD, DWORD, QWORD

Character Sets

- ASCII (American Standard Code for Information Interchange)
  - The most widely used character set
  - 7-bit
  - Represent 128 numbers, letters, punctuation marks, and other symbols.
    - Standard English keyboard
  - Full list at http://www.neurophys.wisc.edu/comp/docs/ascii/
- Extended ASCII
  - 8 bit
  - Standard ASCII character set, plus additional characters
    - For example €, ƒ, Æ, ™, ©

ASCII

Dec	Hx	Oct	Char	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr	Dec	Hx	Oct	Html	Chr
0	0	000	NUL (null)	32	20	040		Space	64	40	100	@	@	96	60	140	`	`
1	1	001	SOH (start of heading)	33	21	041	!	!	65	41	101	A	A	97	61	141	a	a
2	2	002	STX (start of text)	34	22	042	"	"	66	42	102	B	B	98	62	142	b	b
3	3	003	ETX (end of text)	35	23	043	#	#	67	43	103	C	C	99	63	143	c	c
4	4	004	EOT (end of transmission)	36	24	044	$	$	68	44	104	D	D	100	64	144	d	d
5	5	005	ENQ (enquiry)	37	25	045	%	%	69	45	105	E	E	101	65	145	e	e
6	6	006	ACK (acknowledge)	38	26	046	&	&	70	46	106	F	F	102	66	146	f	f
7	7	007	BEL (bell)	39	27	047	'	'	71	47	107	G	G	103	67	147	g	g
8	8	010	BS (backspace)	40	28	050	(	(	72	48	110	H	H	104	68	150	h	h
9	9	011	TAB (horizontal tab)	41	29	051	)	)	73	49	111	I	I	105	69	151	i	i
10	A	012	LF (NL line feed, new line)	42	2A	052	*	*	74	4A	112	J	J	106	6A	152	j	j
11	B	013	VT (vertical tab)	43	2B	053	+	+	75	4B	113	K	K	107	6B	153	k	k
12	C	014	FF (NP form feed, new page)	44	2C	054	,	,	76	4C	114	L	L	108	6C	154	l	l
13	D	015	CR (carriage return)	45	2D	055	-	-	77	4D	115	M	M	109	6D	155	m	m
14	E	016	SO (shift out)	46	2E	056	.	.	78	4E	116	N	N	110	6E	156	n	n
15	F	017	SI (shift in)	47	2F	057	/	/	79	4F	117	O	O	111	6F	157	o	o
16	10	020	DLE (data link escape)	48	30	060	0	0	80	50	120	P	P	112	70	160	p	p
17	11	021	DC1 (device control 1)	49	31	061	1	1	81	51	121	Q	Q	113	71	161	q	q
18	12	022	DC2 (device control 2)	50	32	062	2	2	82	52	122	R	R	114	72	162	r	r
19	13	023	DC3 (device control 3)	51	33	063	3	3	83	53	123	S	S	115	73	163	s	s
20	14	024	DC4 (device control 4)	52	34	064	4	4	84	54	124	T	T	116	74	164	t	t
21	15	025	NAK (negative acknowledge)	53	35	065	5	5	85	55	125	U	U	117	75	165	u	u
22	16	026	SYN (synchronous idle)	54	36	066	6	6	86	56	126	V	V	118	76	166	v	v
23	17	027	ETB (end of trans. block)	55	37	067	7	7	87	57	127	W	W	119	77	167	w	w
24	18	030	CAN (cancel)	56	38	070	8	8	88	58	130	X	X	120	78	170	x	x
25	19	031	EM (end of medium)	57	39	071	9	9	89	59	131	Y	Y	121	79	171	y	y
26	1A	032	SUB (substitute)	58	3A	072	:	:	90	5A	132	Z	Z	122	7A	172	z	z
27	1B	033	ESC (escape)	59	3B	073	;	;	91	5B	133	[	[	123	7B	173	{	{
28	1C	034	FS (file separator)	60	3C	074	<	<	92	5C	134	\	\	124	7C	174			|
29	1D	035	GS (group separator)	61	3D	075	=	=	93	5D	135	]	]	125	7D	175	}	}
30	1E	036	RS (record separator)	62	3E	076	>	>	94	5E	136	^	^	126	7E	176	~	~
31	1F	037	US (unit separator)	63	3F	077	?	?	95	5F	137	_	_	127	7F	177	&#127;	DEL

Source: www.LookupTables.com

Examples

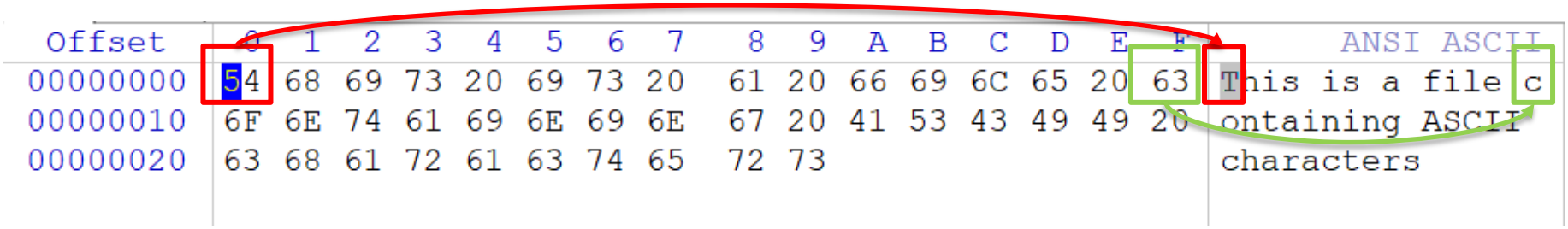
- Q1. What is the Hexadecimal representation (using the ASCII character set) of the string “Lab”?
- A1. 4C6162
- Q2. What ASCII character is represented by decimal 63?
- A2. ?

Character Sets

- Unicode
  - 16 bit
  - Foreign languages
  - Emojis

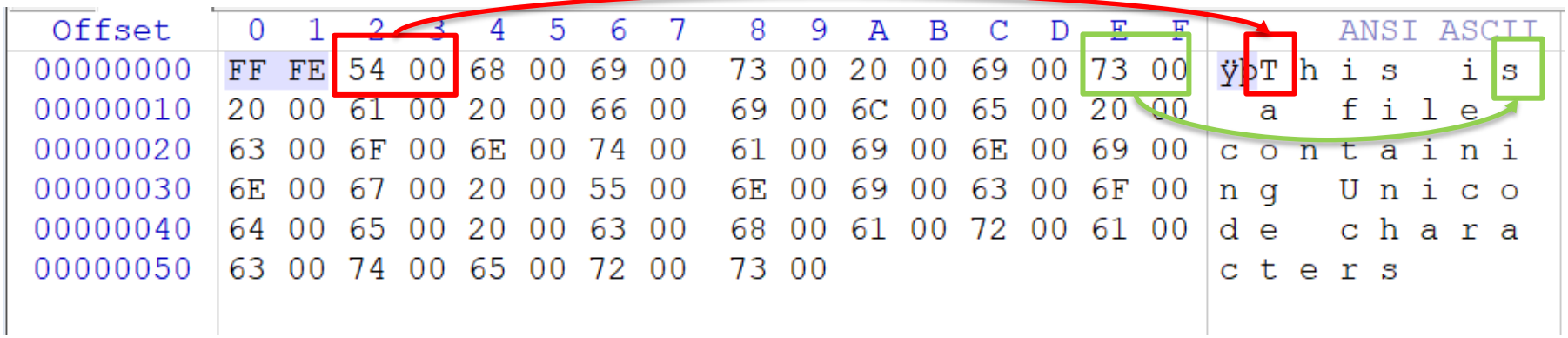
Hexadecimal and ASCII/Unicode

- ASCII



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	54	68	69	73	20	69	73	20	61	20	66	69	6C	65	20	63	This is a file c
00000010	6F	6E	74	61	69	6E	69	6E	67	20	41	53	43	49	49	20	ontaining ASCII
00000020	63	68	61	72	61	63	74	65	72	73							characters

- Unicode



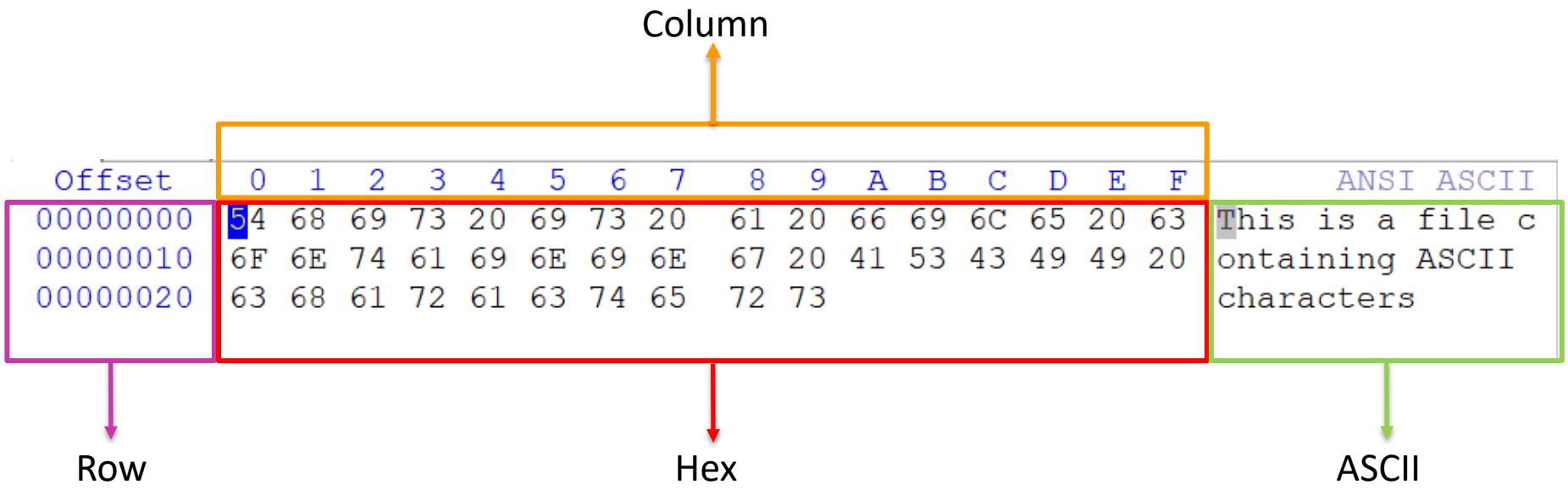
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	FF	FE	54	00	68	00	69	00	73	00	20	00	69	00	73	00	ÿþT h i s i s
00000010	20	00	61	00	20	00	66	00	69	00	6C	00	65	00	20	00	a f i l e
00000020	63	00	6F	00	6E	00	74	00	61	00	69	00	6E	00	69	00	c o n t a i n i
00000030	6E	00	67	00	20	00	55	00	6E	00	69	00	63	00	6F	00	n g U n i c o
00000040	64	00	65	00	20	00	63	00	68	00	61	00	72	00	61	00	d e c h a r a
00000050	63	00	74	00	65	00	72	00	73	00							c t e r s

00 = NUL

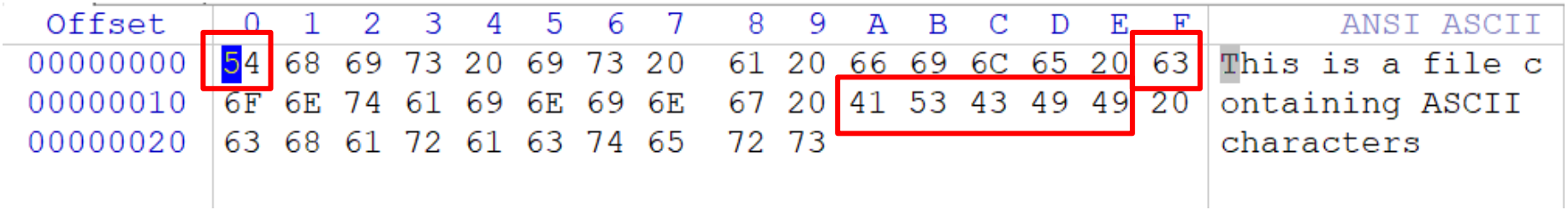
Offset

- A way to address or reference data with a disk/file
- Physical Offset
  - From the beginning of the disk
- Logical Offset
  - From the beginning of the partition/file

Offset



Offset Examples



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	54	68	69	73	20	69	73	20	61	20	66	69	6C	65	20	63	This is a file c
00000010	6F	6E	74	61	69	6E	69	6E	67	20	41	53	43	49	49	20	ontaining ASCII
00000020	63	68	61	72	61	63	74	65	72	73							characters

- Offset 00
  - 54h or T
- Offset 0F
  - 63h or c
- Offset 1A for length of 5
  - 4153434949h or ASCII

Offset Examples

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000160	0D	0A	61	0D	0A	61	0D	0A	61	0D	0A	61	0D	0A	61	0D	a a a a a
00000170	0A	61	0D	0A	61	0D	0A	61	0D	0A	54	68	69	73	20	69	a a a This i
00000180	73	20	61	20	66	69	6C	65	20	63	6F	6E	74	61	69	6E	s a file contain
00000190	69	6E	67	20	41	53	43	49	49	20	63	68	61	72	61	63	ing ASCII charac
000001A0	74	65	72	73													ters

- Offset 190
  - 69h or i
- Offset 1A3
  - 73h or s

Key Learnings

- When dealing with number systems we starting counting from 0, not from 1
- 1 ASCII character (1 byte) is represented by 2 hex characters
  - ASCII L = 4Ch
- Hexadecimal is often written with either 0x prefix or h suffix
  - 0x4C6162
  - 4C6162h
- Uppercase and lowercase characters have different hexadecimal values
  - L = 4Ch, l = 6Ch

The Personal Computer

- To carry out computer forensics an understanding of a typical computer system is necessary
- A “computer system” is made up of hardware and software
  - Hardware – Computer Hardware is the physical equipment such as the case, power supply, motherboard, CPU, memory, disk-drives, keyboards, monitors, mouse, cables, speakers…
  - Software – Computer Software is the operating system and programs

Motherboard

- Main printed circuit board
- Enables communications between different components of the computer, via Buses
- Provides accommodation (seating) for CPU, memory, expansion slots, BIOS chip, sockets, connectors and the like

Central Processing Unit

- Carries out the instructions given to it from the Operating System or from a user written program
- Single, Dual, Quad core chips
- 32 bit and 64 bit instruction sets
  - Issues with forensic tools

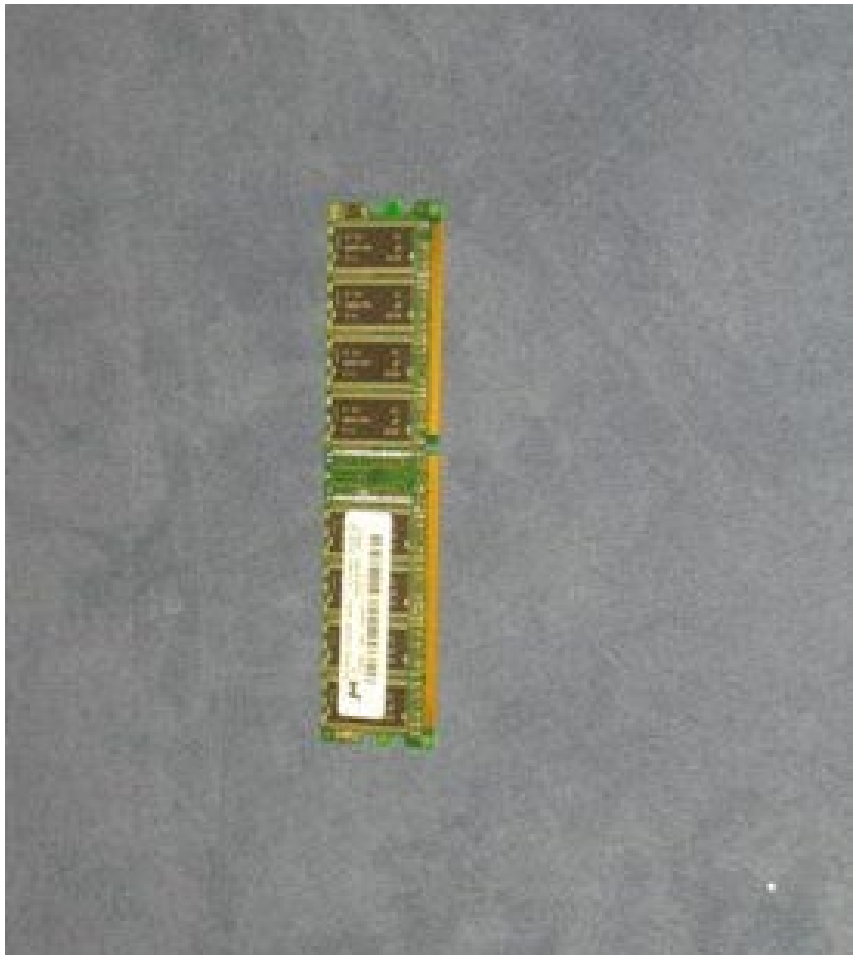
Intel® Core™ i7 processor

SWINBURNE UNIVERSITY OF TECHNOLOGY

.mage Source: https://www.intel.com/pressroom/archive/releases/2008/20081117comp_sm.htm

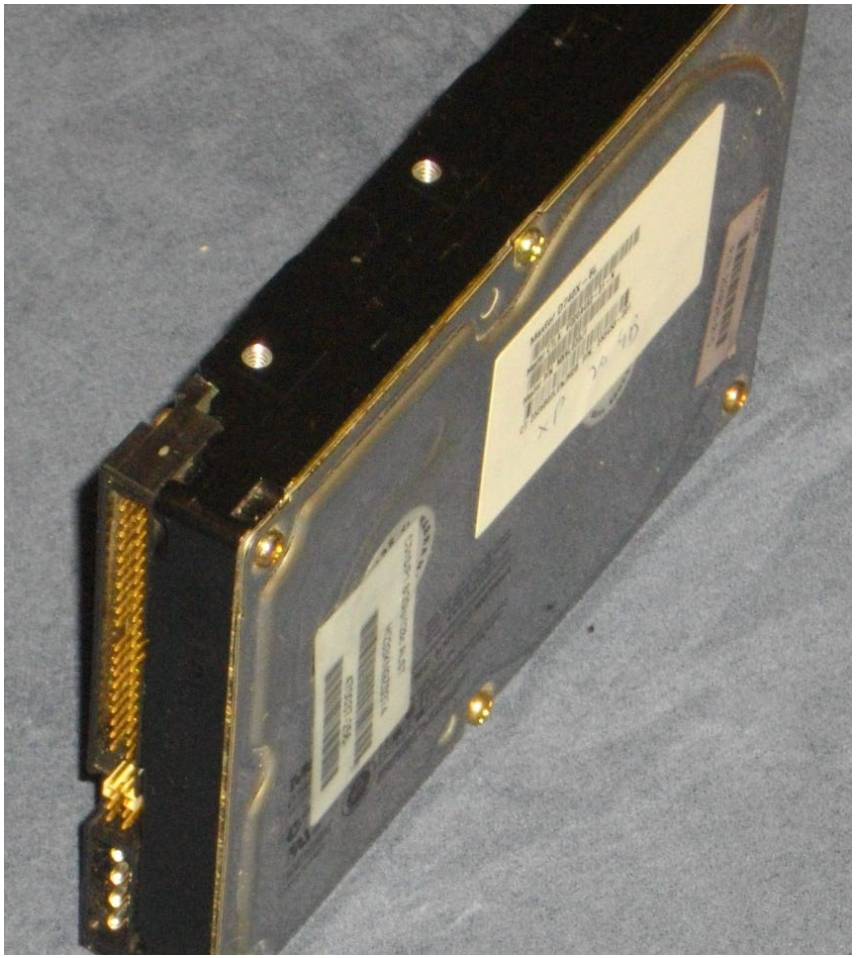
Memory

- Random Access Memory (RAM)
  - Temporary storage for data and programs
  - Contents change as program executes
- Read Only Memory (ROM)
  - Located on motherboard
  - Unchanging



Storage Devices: Hard Drives

- Magnetic storage device
- Used for permanent storage of data
- Usually mapped in Windows to c:\
- Contained within the computer case (usually) although external drives can be connected via USB

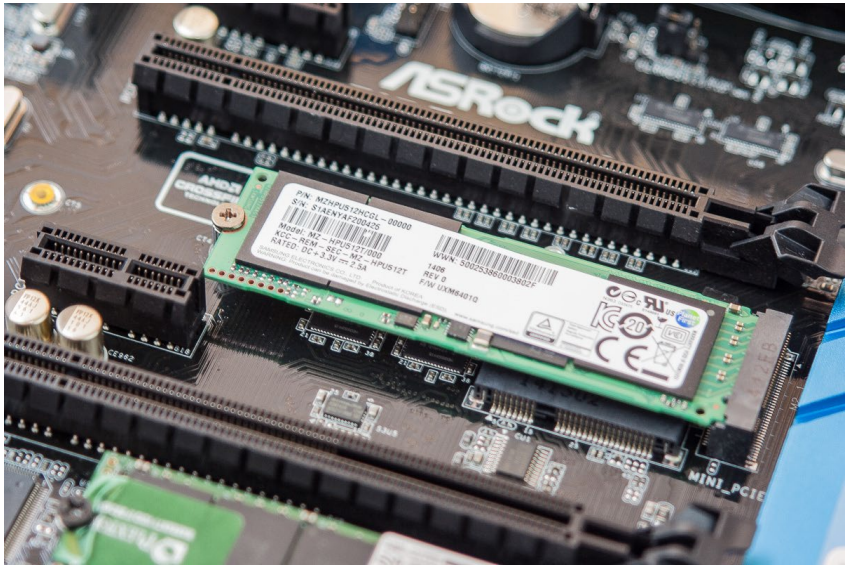


Storage Devices: Solid State Drives

- PCI Express

http://blazinglist.com/wp-content/uploads/2015/12/Top-7-Best-PCI-Express-PCIe-SSD-Drives-In-2016-1-696x329.jpg

- M.2



http://media.bestofmicro.com/E/D/435973/original/IMG_0754-1.jpg

Storage Devices: Optical Drives

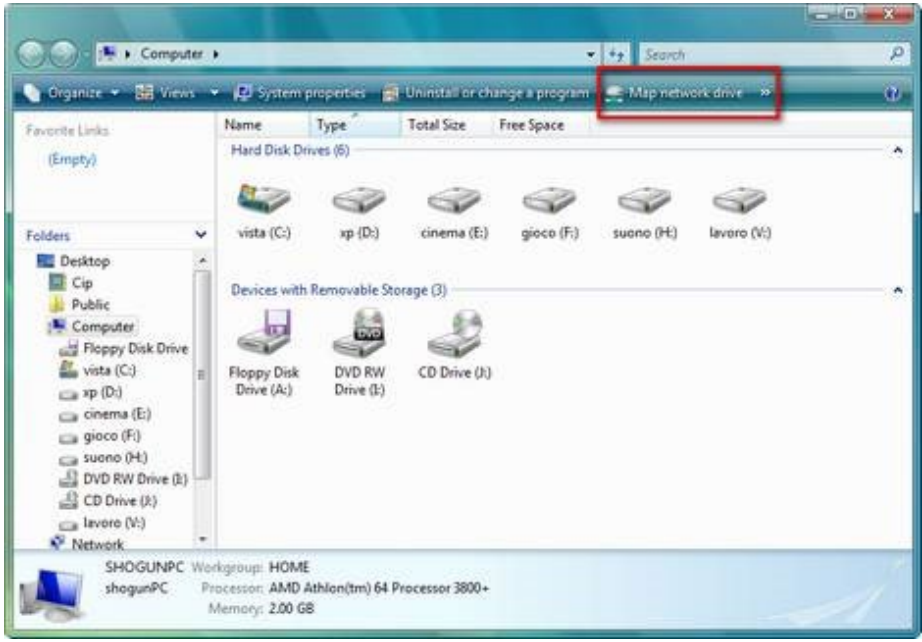
- Compact Disk (CD)
- Digital Versatile Disk (DVD)
- Blu-ray Disc (BD)
- Usually mapped in Windows to d:\
- Numerous versions
  - CD-ROM
  - CD-R
  - DVD-ROM
  - DVD+/-R
  - …and a few others

Storage Devices: Flash Drives

- Removable storage device that connects via the USB port
- Replaced FDDs
- Typically 32 to 256 GB of storage, some 2TB +
- Usually mapped in Windows to e:\ or f:\
- (picture from techninfor-4u.com)

Storage Devices: Network Drives

- Storage device that mimics the behaviour of a local hard disk drive but is located on the network
- In Windows usually mapped to a character later in the alphabet such as g:\
- Also “cloud” storage
- Picture from Vista4beginners.com



Adapter Cards

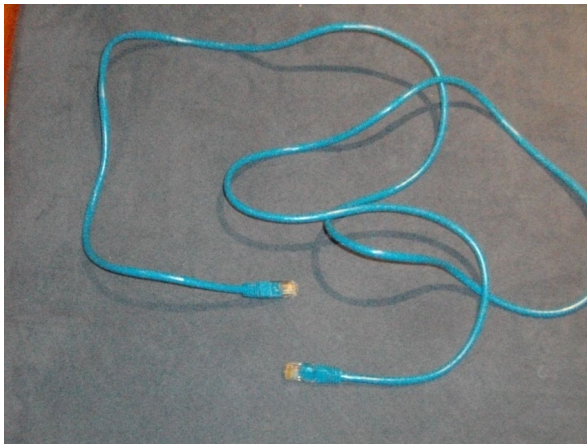
- Network Interface Cards (NICs)
  - RJ-45 interface
  - Ethernet most common protocol
  - Often built-in to the motherboard
- Video adapter cards
  - VGA, HDMI, DVI, DP, Composite and Component Video, S-Video common standards

Motherboard Ports

- Image Source: https://www.quora.com/What-are-the-ports-on-the-motherboard-and-their-functions

Network Interfaces

- UTP – straight through
  - In Ethernet is used to connect a host to a switch and a switch to a router
- UTP – cross over
  - In Ethernet is used to connect a host to a router or two of the same devices (eg host to host or switch to switch)
- Serial
  - Used to connect to modem or other WAN device
- Fibre
  - Connect network switches
  - Servers to storage arrays
- WiFi



Operating Systems

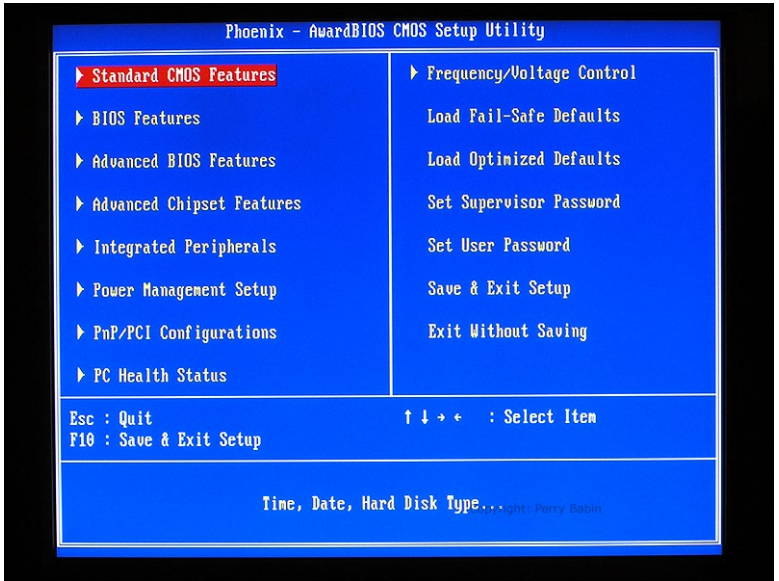
- BIOS – Basic Input/Output System
- Microsoft Windows
- Linux
- Apple MacOS (OS X)
- Mobile OS (iOS / Android)
- GUI interfaces v Command line interfaces

Operating System Functions

- Hardware access
- User interface
- File management
- Application program management

Basic Input/Output System (BIOS)

- Built into the PC
  - Contained on a ROM chip seated on the Motherboard
- First action of PC after Power On Self Test is to run the BIOS
- The BIOS usually loads an Operating System (Windows, Linux, MacOS) from one of the storage devices
- OS load can be interrupted and some basic functions carried out within the BIOS
- Trustedreviews.com and bcot1.com



Microsoft Windows

- Most widely used Desktop Operating System in the world
- Has evolved through a number of different releases
  - Windows 1,2,3, Windows NT, Windows 95 – ran “on top of” DOS
  - Windows 98, Windows 2000, Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10
- Home user versions and server versions for businesses
- Graphical User Interface but with command line interface options

Linux

- Open source operating system
- Unix for PCs
- Different distributions (Debian, Ubuntu, Centos, Red Hat, openSuse)
  - Same underlying Linux kernel
  - Desktop and Server distribution
  - Desktop may include KDE or GNOME
- GUI and command line interfaces

Apple Mac OS

- Apple Inc OS for the Macintosh
- Originally no Command Line Interface
  - Solely Graphical User Interface
- MacOS for older PowerPC hardware
- OSX for intel hardware based on OpenBSD (Unix)

Conclusion

- Overview of number systems
- Overview of character sets
- Units of Measurement
- PC hardware and operating systems