Topic 2 Evidence in computers and networks Part 1

Learning Outcome

- After successfully completing this lecture, you will be able to
  - Describe evidence in computers and networks

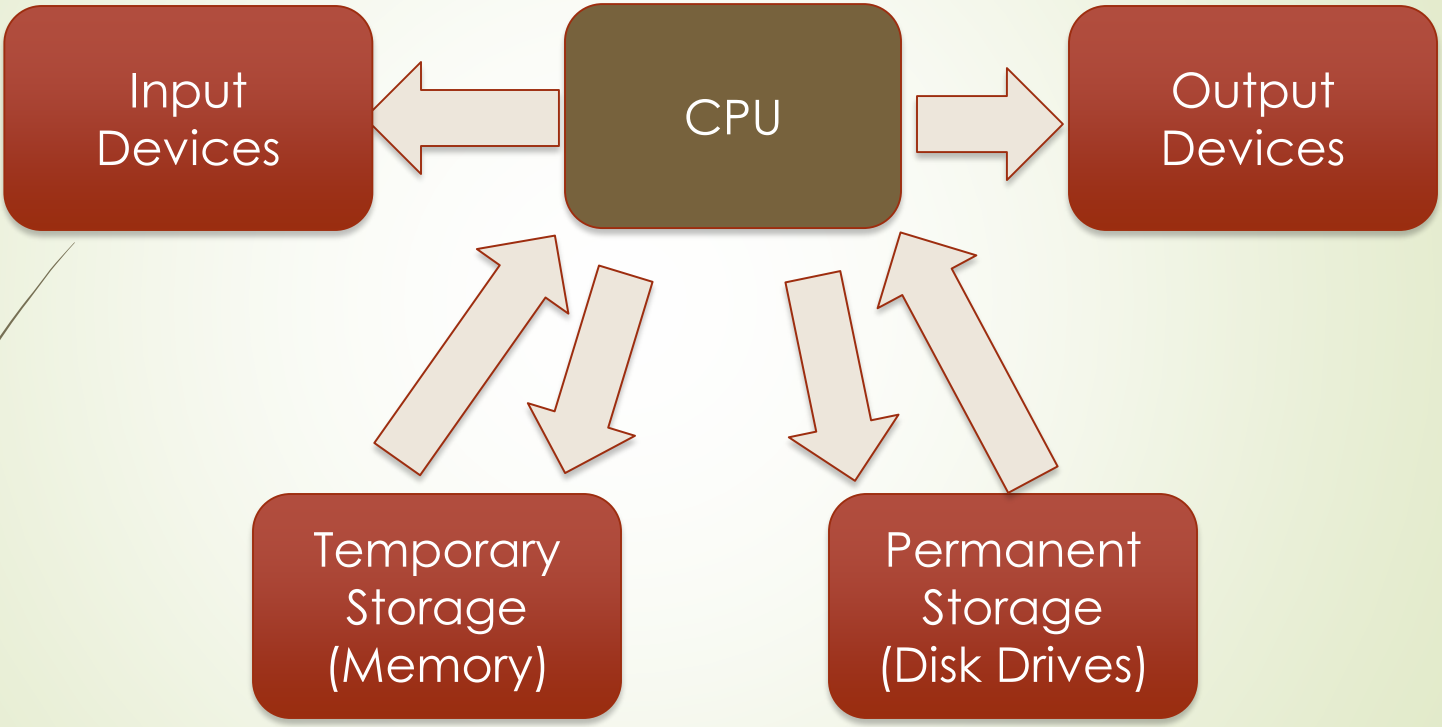
Road Map

- Evidence in computers and networks
- File systems
- Computer memory
- Network connections
- Network event logs

Evidence in computers and networks

- Evidence in computers
  - File systems
  - Operating systems
  - Application
  - Computer memory
- Evidence in networks
  - Network traffic
  - Event logs in network devices
    - Routers
    - LAN switches
    - Firewalls
    - Web, Proxy, DNS, Proxy, DNS and Windows Directory domain controllers

Evidence in computers – computer architecture



Q1: Which storage in a computer is volatile?

a) BIOS
b) Memory
c) Hard disk drive
d) USB remote drive
e) Cloud storage
f) Keyboard

See Answer in the last slide of this lecture note

Q1: Which storage in a computer is volatile?

a) BIOS

b) Memory

c) Hard disk drive

d) USB remote drive

e) Cloud storage

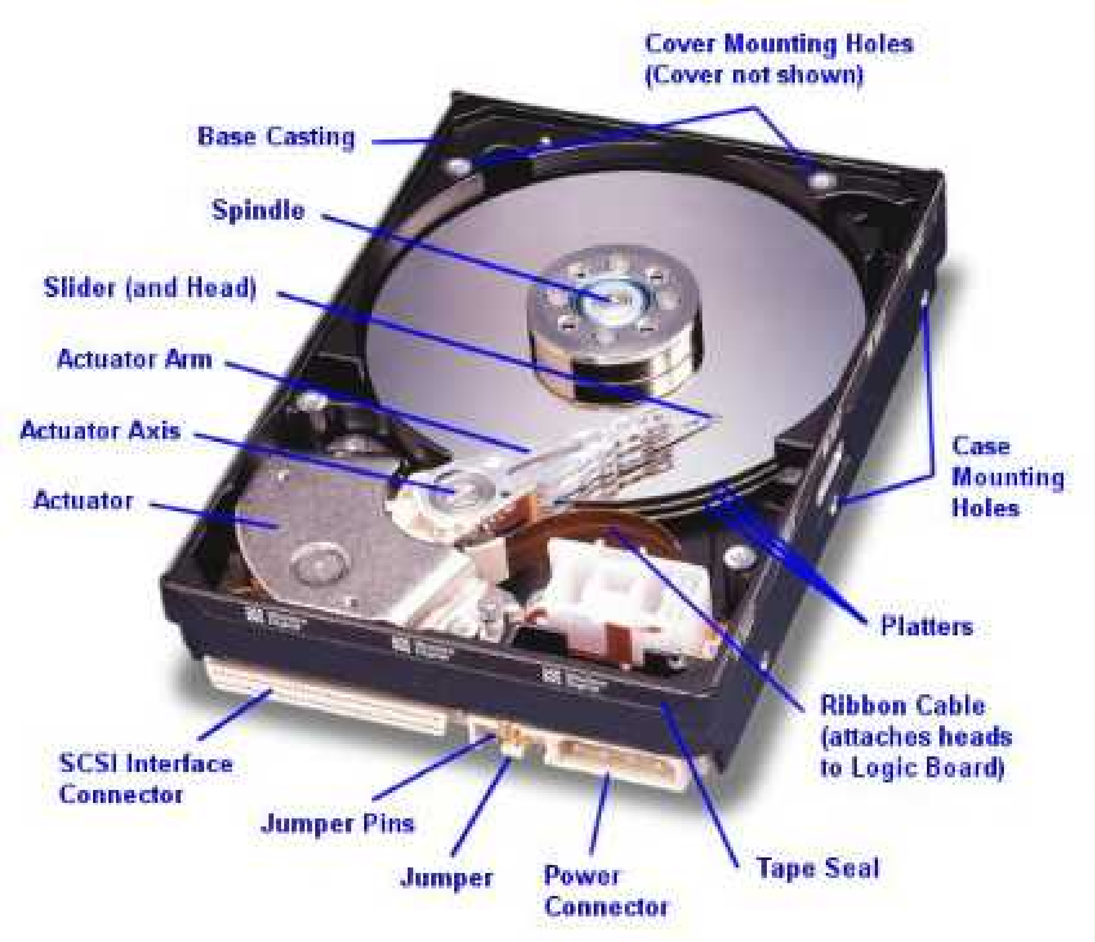
f) Keyboard

See Answer in the last slide of this lecture note

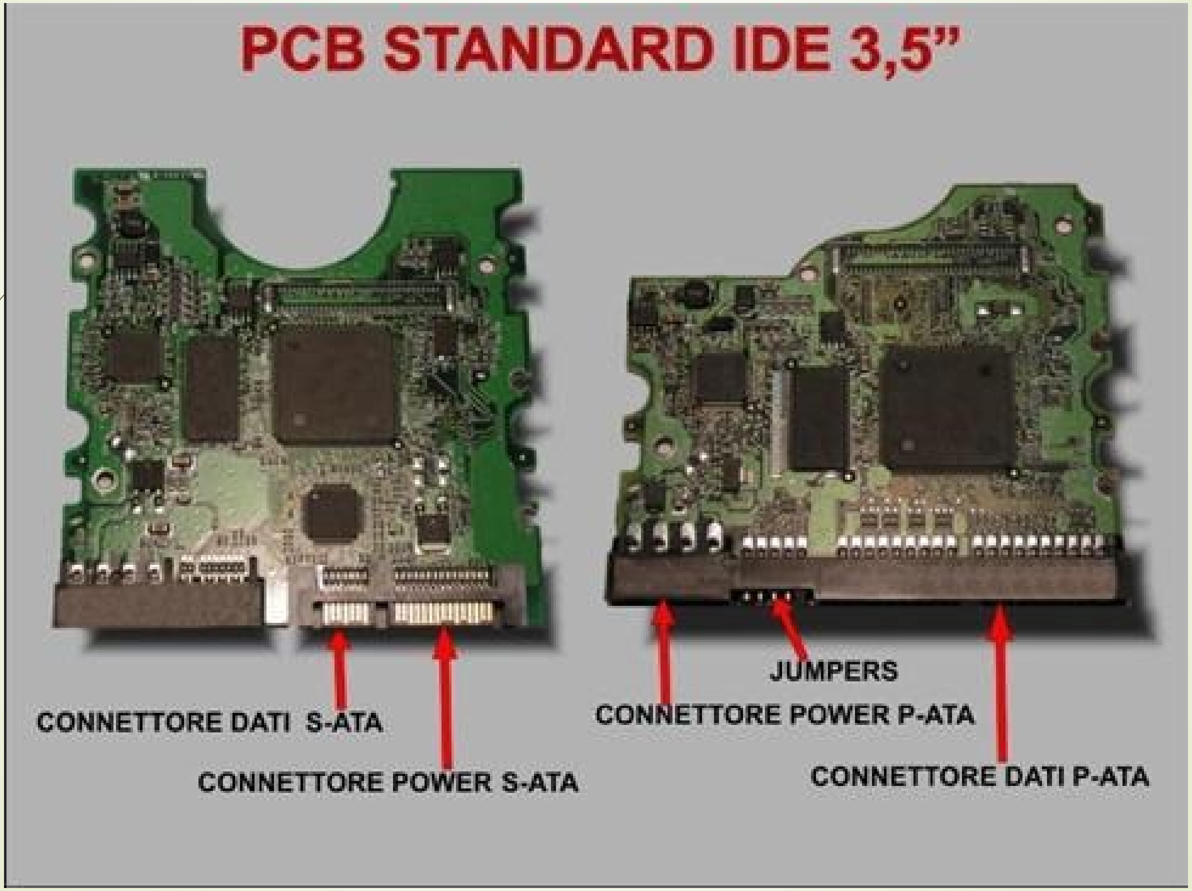
Hard Disk Storage

- Head Disk Assembly
- Control Logic and Computer Interface Circuit Board
- Computer Interface Standards
  - Internal hard disk drive interface
    - IDE and SATA
  - External hard disk drive interface
    - SCSI and USB
- Redundant array of independent disks (RAID)

Head Disk Assembly

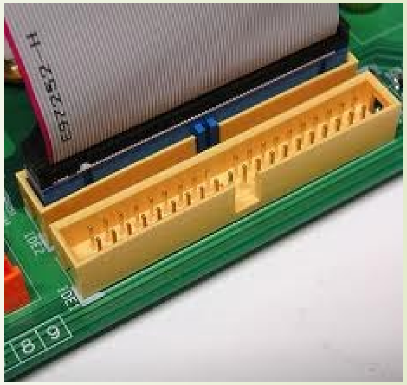


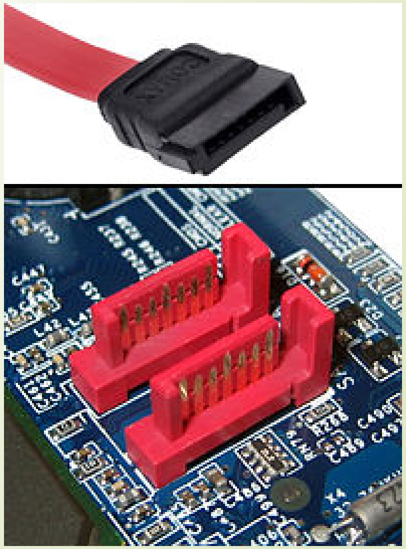
Control Logic and Computer Interface Circuit Board



Internal hard disk interfaces IDE and SATA Interface

- IDE
  - It is a 16-bit parallel data bus that connects disk drive to the 16-bit data bus of PC at a speed of 133MB/s
- SATA (Serial AT Attachment)
  - SATA 3.0 provide a serial data bit transfer rate at 6 Gbps (gigabit/s) or 750MB/s





External hard disk interfaces SCSI and USB

- SCSI (Small Computer System Interface) was used for interfacing external hard drives from 1984 to 2003. The maximum speed is 640MB/s
- USB (Universal Serial Bus) started from 1996. The current version USB 3.0 (2008) has a maximum speed of 625MB/s
- USB Type C started from 2017. 40Gbit/s in Thunderbolt mode, 10Gbit/s in USB 3.1 mode

(photo by Santeri Viinamäki - https://commons.wikimedia.org/wiki/File:USB_Type-C_plug_20170626.jpg?uselang=fr, CC BY-SA 4.0)

Q2: Which is internal storage interface standard?

a) USB

b) RS232C

c) Fibre channel

d) SATA

See Answer in the last slide of this lecture note

Q2: Which is internal storage interface standard?

a) USB

b) RS232C

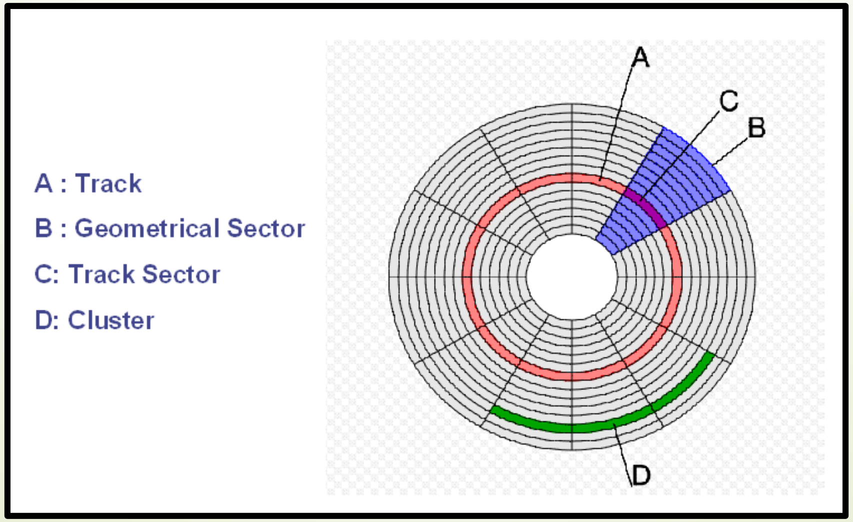
c) Fibre channel

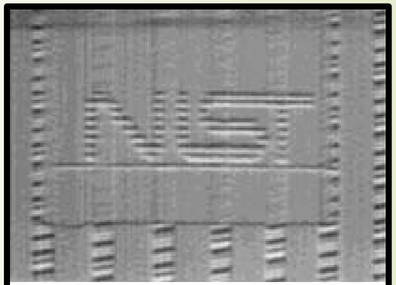
d) SATA

See Answer in the last slide of this lecture note

File System Abstraction Model

- Disk
  - Physical storage device (e.g. SCSI or SATA hard drive)
  - Physical analysis beyond the capability of most examiners





This image from the second harmonic magneto-resistive microscope shows portions of six tracks on a hard drive that were overwritten with the NIST logo. The overwritten portions are faintly visible.

Source: NIST

Hard Disk Drive Technical Terms

- Sector
  - A data block on disk surface storing 516 bytes of date
- Track
  - A circular track on disk surface consist of 63 sectors
- Cluster
  - A collection of 16 consecutive sectors (4,096 bytes) on a track. OS likes Windows allocate minimum 1 cluster per file.
- Head
  - Magnetic read/write head flying over a specific track
- Cylinder
  - A collection of heads flying over the same track number on respective disk surface

Q3: A hard disk drive has 5 read/write heads, 1,000 cylinders and 64 sector per track. What is the total storage of this drive?

a) 5,000 bytes
b) 64,000 bytes
c) 320,000 bytes
d) 163,840,000 bytes

See Answer in the last slide of this lecture note

Q3: A hard disk drive has 5 read/write heads, 1,000 cylinders and 64 sector per track. What is the total storage of this drive?

a) 5,000 bytes

b) 64,000 bytes

c) 320,000 bytes

d) 163,840,000 bytes

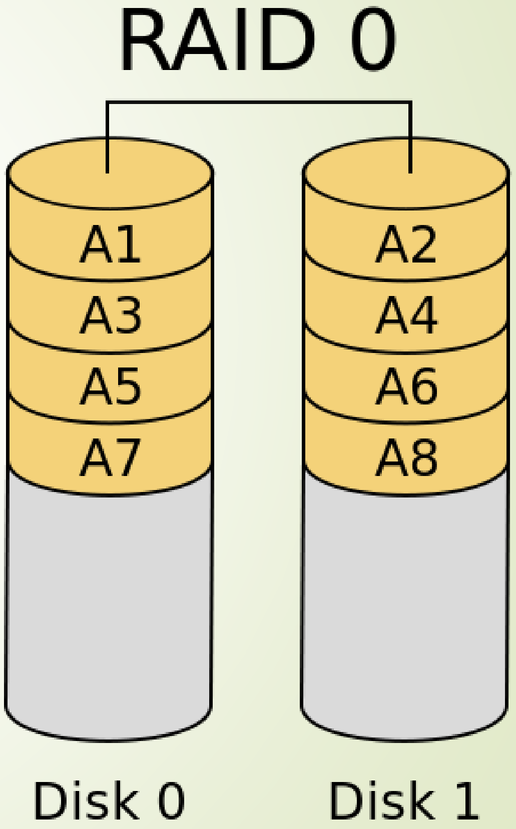
See Answer in the last slide of this lecture note

File System Abstraction Model

- Partition
  - A collection of **physically** consecutive sectors
  - Defined by an entry in the partition table
- Volume
  - A collection of **logically** addressable sectors
  - Defined by the operating system, e.g. C:, D:
  - Contains the file system, e.g. FAT, NTFS

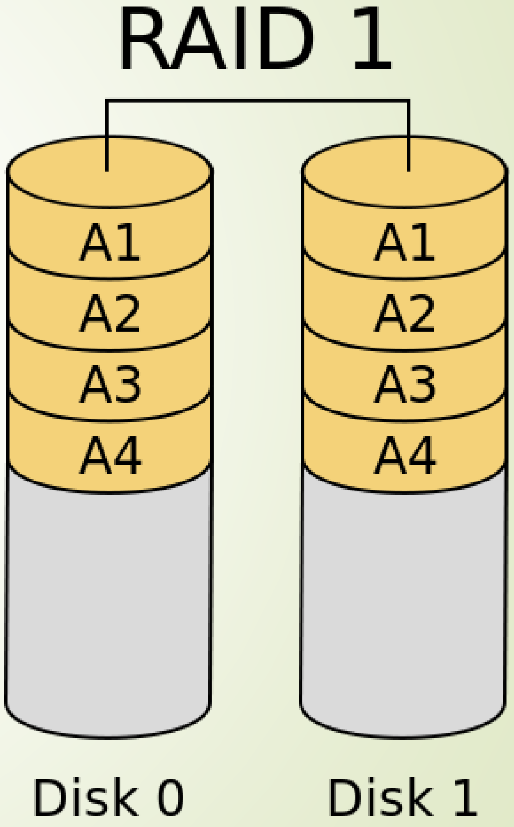
RAID 0 - Improved Performance (redundant array of independent disks)

- RAID 0 (block-level striping without parity or mirroring) has no (or zero) redundancy. It provides improved performance and additional storage but no fault tolerance. Hence simple stripe sets are normally referred to as RAID 0



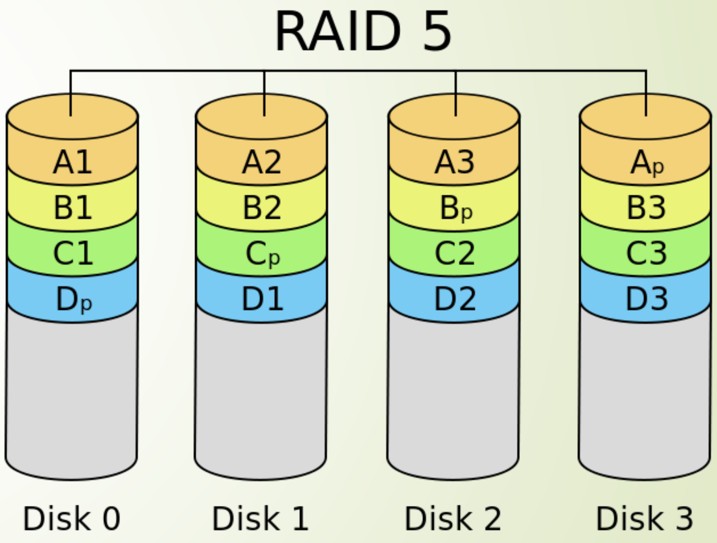
RAID 1 - Mirroring

- RAID I (mirroring without parity or striping), data is written identically to two drives, thereby producing a "mirrored set"; the read request is serviced by either of the two drives containing the requested data, whichever one involves least seek time plus rotational latency.



RAID 5 – Survive on one disk failure

- RAID 5 (block-level striping with distributed parity) distributes parity along with the data and requires all drives but one to be present to operate; the array is not destroyed by a single drive failure. Upon drive failure, any subsequent reads can be calculated from the distributed parity such that the drive failure is masked from the end user.



Q4: Which RAID configuration provides both improved data access speed and single-hard-drive-failure fail-over protection?

a) RAID 0

b) RAID 1

c) RAID 5

See Answer in the last slide of this lecture note

Q4: Which RAID configuration provides both improved data access speed and single-hard-drive-failure fail-over protection?

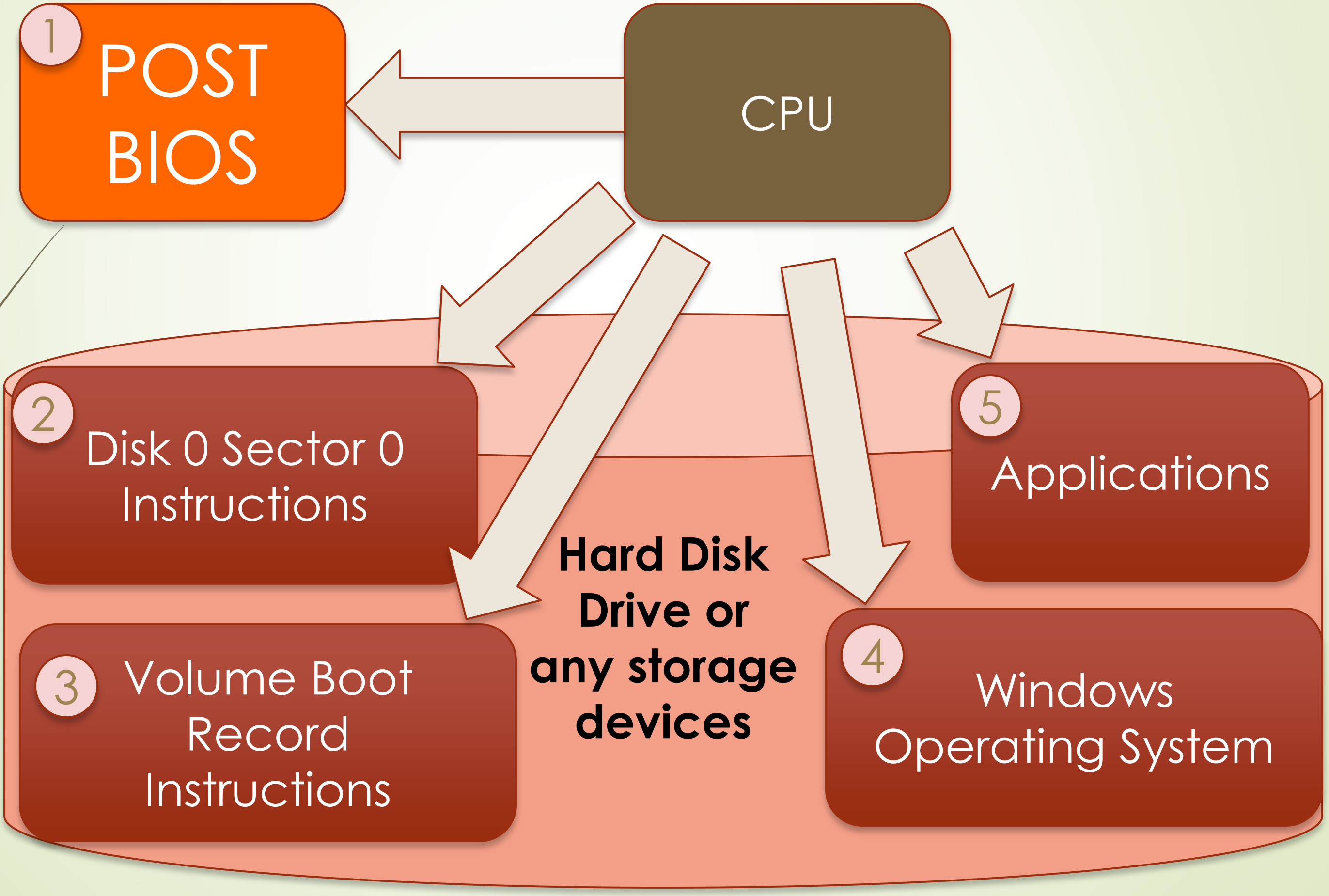
a) RAID 0

b) RAID 1

c) RAID 5

See Answer in the last slide of this lecture note

Evidence in computers – How a computer boot up


1
POST
BIOS
CPU
2
Disk 0 Sector 0 Instructions
3
Volume Boot Record Instructions
Hard Disk Drive or any storage devices
4
Windows Operating System
5
Applications

The Computer Boot Process

- POST – Power On Self Test
  - Self-diagnostic programme to test hardware components: CPU, RAM, I/O devices
- BIOS – Basic Input Output System
  - Prepare the system to a state of operational readiness
    - Enumerate, test and initialise peripheral devices (keyboard, mouse, disk drives, printer video cards etc)
    - Load the operating system into main memory
  - Hard disk content may be altered if it's not write-protected
    - Files are accessed resulted in the change of metadata like file access and modification time

The Computer Boot Process

- BIOS/CMOS setup
  - Programme to display and edit user configurable settings in the BIOS
    - System clock
      - Weak CMOS battery can lead to inaccurate system time
    - Boot sequence
      - Need to prevent the computer from booting up the evidence drive
- MBR – Master Boot Record for BIOS system
  - Located at the 1st sector of the 1st drive in the boot sequence in BIOS
    - Master boot code
    - Disk signature
    - Partition table

Q5: After a computer is powered up, which instruction will be read first just before loading Windows OS system into the memory?

a) Windows kernel instructions

b) BIOS

c) Volume boot record instructions

d) POST

See Answer in the last slide of this lecture note

Q5: After a computer is powered up, which instruction will be read first just before loading Windows OS system into the memory?

a) Windows kernel instructions

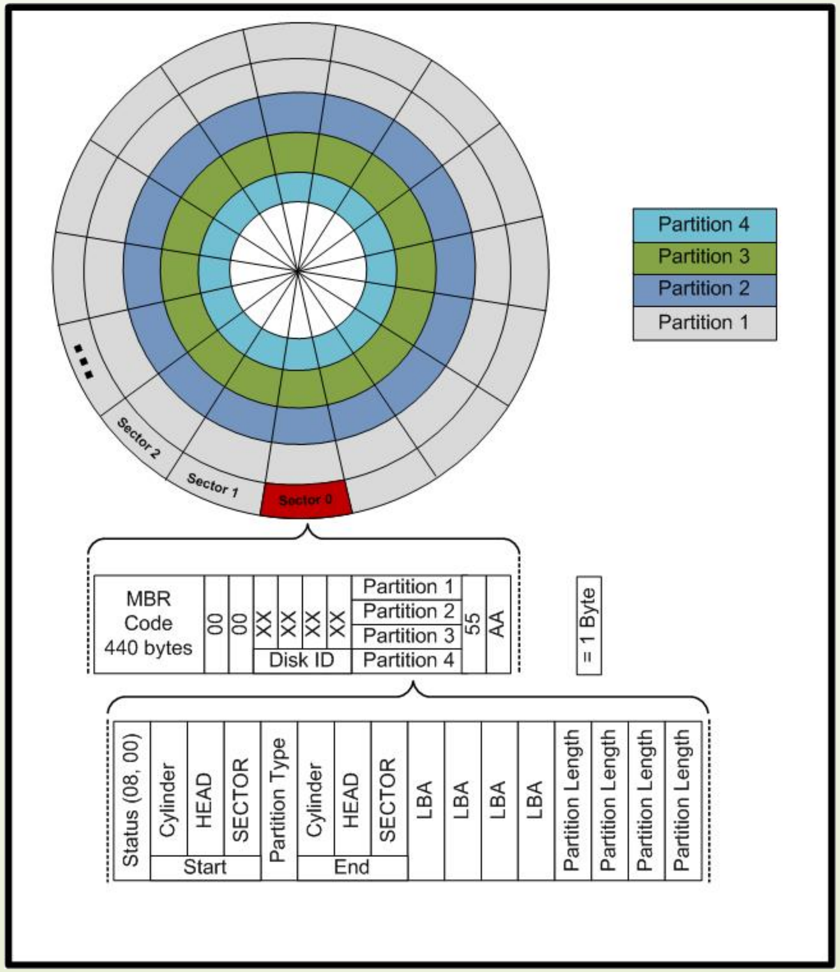
b) BIOS

c) Volume boot record instructions

d) POST

See Answer in the last slide of this lecture note

Where is Master Boot Record?



Structure of a generic MBR (in sector 0 of a physical drive)

Offset	Description	Size in bytes
0x000	Bootstrap Code Area	446
0x1BE	Partition entry #1	16
0x1CE	Partition entry #2	16
0x1DE	Partition entry #3	16
0x1EE	Partition entry #4	16
0x1FE	0x55	1
0x1A	0xAA	1

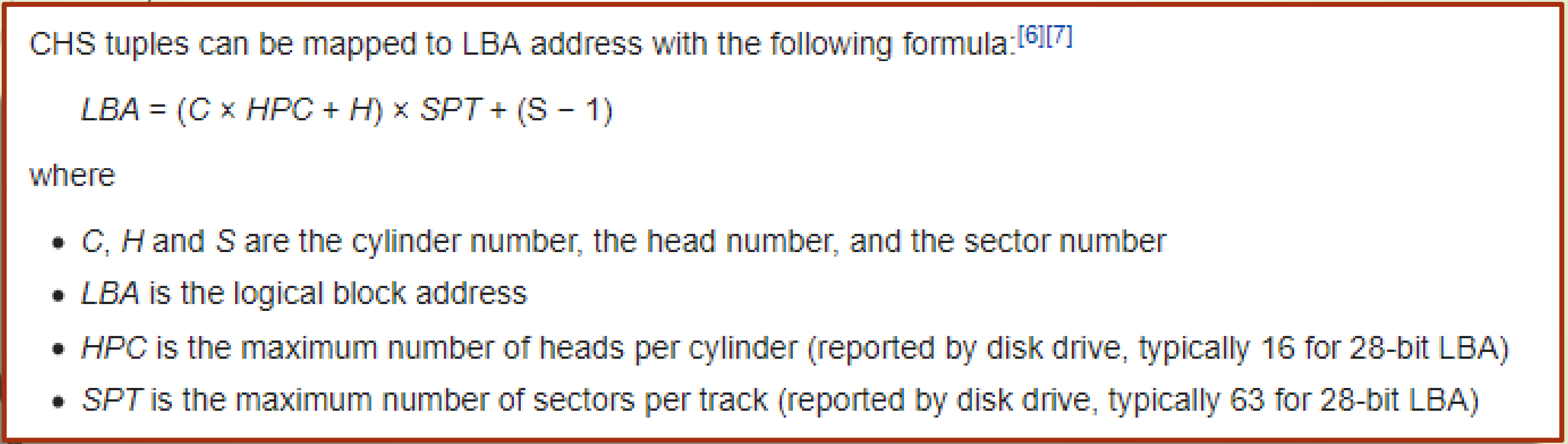
A Sample Partition Entry

Offset	Description	Size in bytes
0x0	0x80 Active or 0x00 Inactive	1
0x1	CHS address of the 1st sector in partition	3
0x4	Partition Type e.g. 0x04 means it is a FAT16 partition	1
0x5	CHS address of last sector in the partition	3
0x8	LBA of the 1st sector in the partition	4
0xC	Number of sectors in the partition	4

Here we know the value of n is the LBA of the 1st sector

What is LBA (Logical Block Address)?

- LBA helps to map sequential, continuous logical blocks to the actual (physical) location of the block at a specific CHS (Cylinder number, Head number and Sector number)



CHS tuples can be mapped to LBA address with the following formula:[6][7]

$$LBA = (C \times HPC + H) \times SPT + (S - 1)$$

where

- *C*, *H* and *S* are the cylinder number, the head number, and the sector number
- *LBA* is the logical block address
- *HPC* is the maximum number of heads per cylinder (reported by disk drive, typically 16 for 28-bit LBA)
- *SPT* is the maximum number of sectors per track (reported by disk drive, typically 63 for 28-bit LBA)

Q6: A hard disk drive has a max. 1,000 cylinders per head, 63 sectors per track and 7 read/write heads, and given the formula LBA = (C × HPC + H) × SPT + (S – 1), what is the LBA of the sector at sector 10, cylinder 5 and head 2?

a) 6301
b) 2340
c) 315135
d) 126326

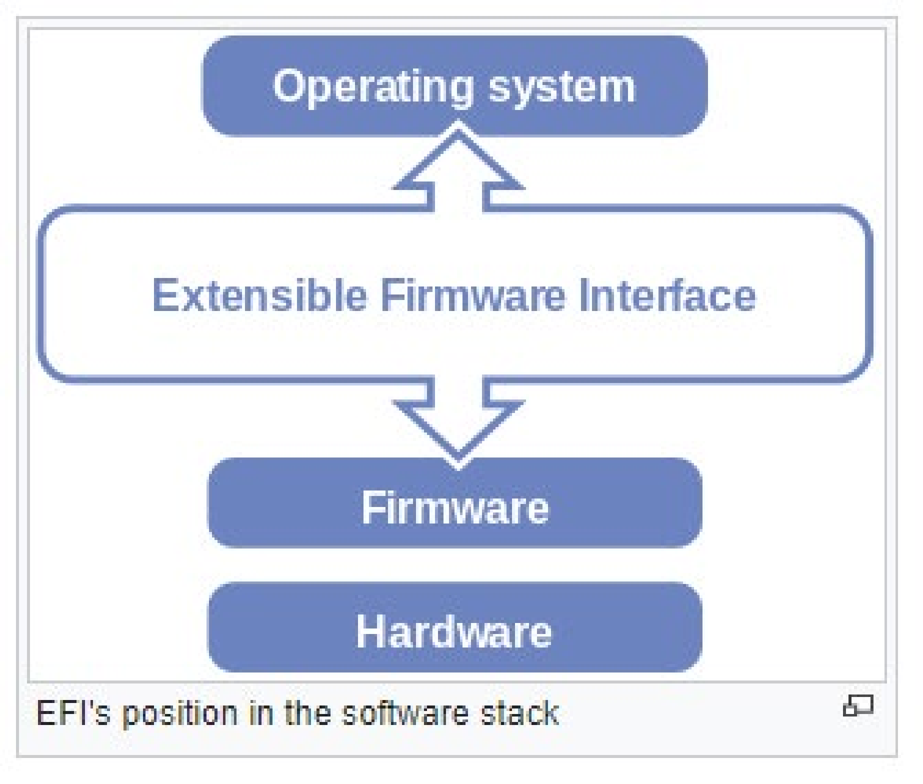
See Answer in the last slide of this lecture note

Q6: A hard disk drive has a max. 1,000 cylinders per head, 63 sectors per track and 7 read/write heads, and given the formula LBA = (C × HPC + H) × SPT + (S – 1), what is the LBA of the sector at sector 10, cylinder 5 and head 2?

a) 6301
b) 2340
c) 315135
d) 126326

See Answer in the last slide of this lecture note

Unified Extensible Firmware Interface (UEFI) replaces BIOS

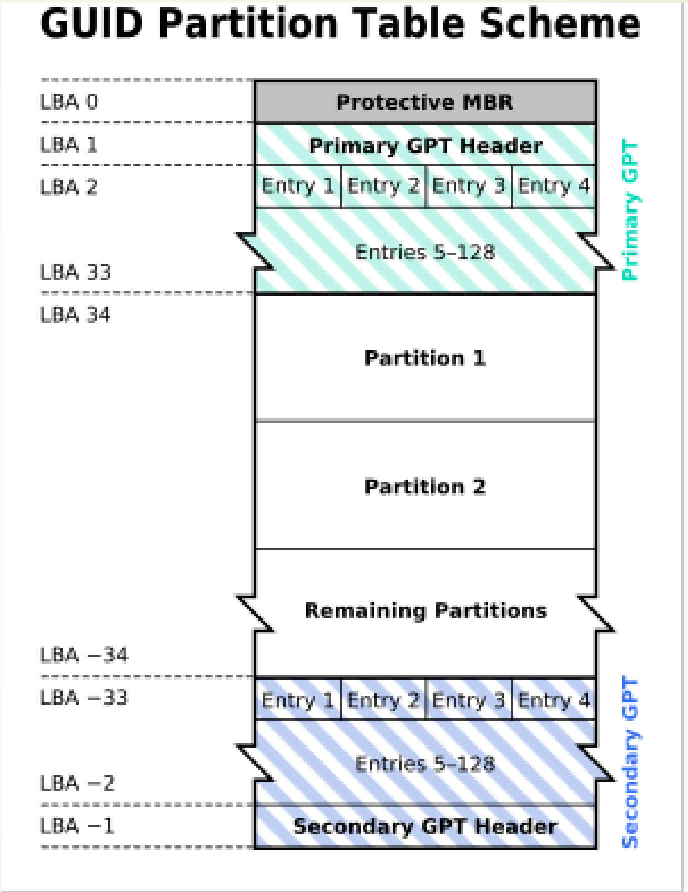


EFI's position in the software stack

UEFI provides legacy support for BIOS services. UEFI can support remote diagnostics and repair of computers, even with no operating system installed

GUID Partition Table (GPT)

Globally **U**nique **Id**entifiers (GUID)



The layout of a disk with the GUID Partition Table. In this example, each logical block is 512 bytes in size and each entry has 128 bytes. The corresponding partition entries are assumed to be located in LBA 2–33. Negative LBA addresses indicate a position from the end of the volume, with −1 being the last addressable block.

GUID Partition Table (GPT)

- The GUID Partition Table (GPT) is a standard for the layout of partition tables of a physical computer storage device, such as a hard disk drive or solid-state drive, using globally unique identifiers (GUIDs).
- It forms a part of the Unified Extensible Firmware Interface (UEFI) standard (Unified EFI Forum-proposed replacement for the PC BIOS), it is nevertheless also used for some BIOS systems, because of the limitations of master boot record (MBR) partition tables, which use 32 bits for logical block addressing (LBA) of traditional 512-byte disk sectors.
- All modern personal computer operating systems support GPT. Some, including macOS and Microsoft Windows on the x86 architecture, support booting from GPT partitions only on systems with EFI firmware, but FreeBSD and most Linux distributions can boot from GPT partitions on systems with both legacy BIOS firmware interface and EFI.

What are advantages of GPT compares with MBR

MBR

- Use 32 bits for block address (LBA)
- Max. size of a partition 2TiB (2^{32} x 512 bytes/block)
- Limited to 4 partitions in a physical drive

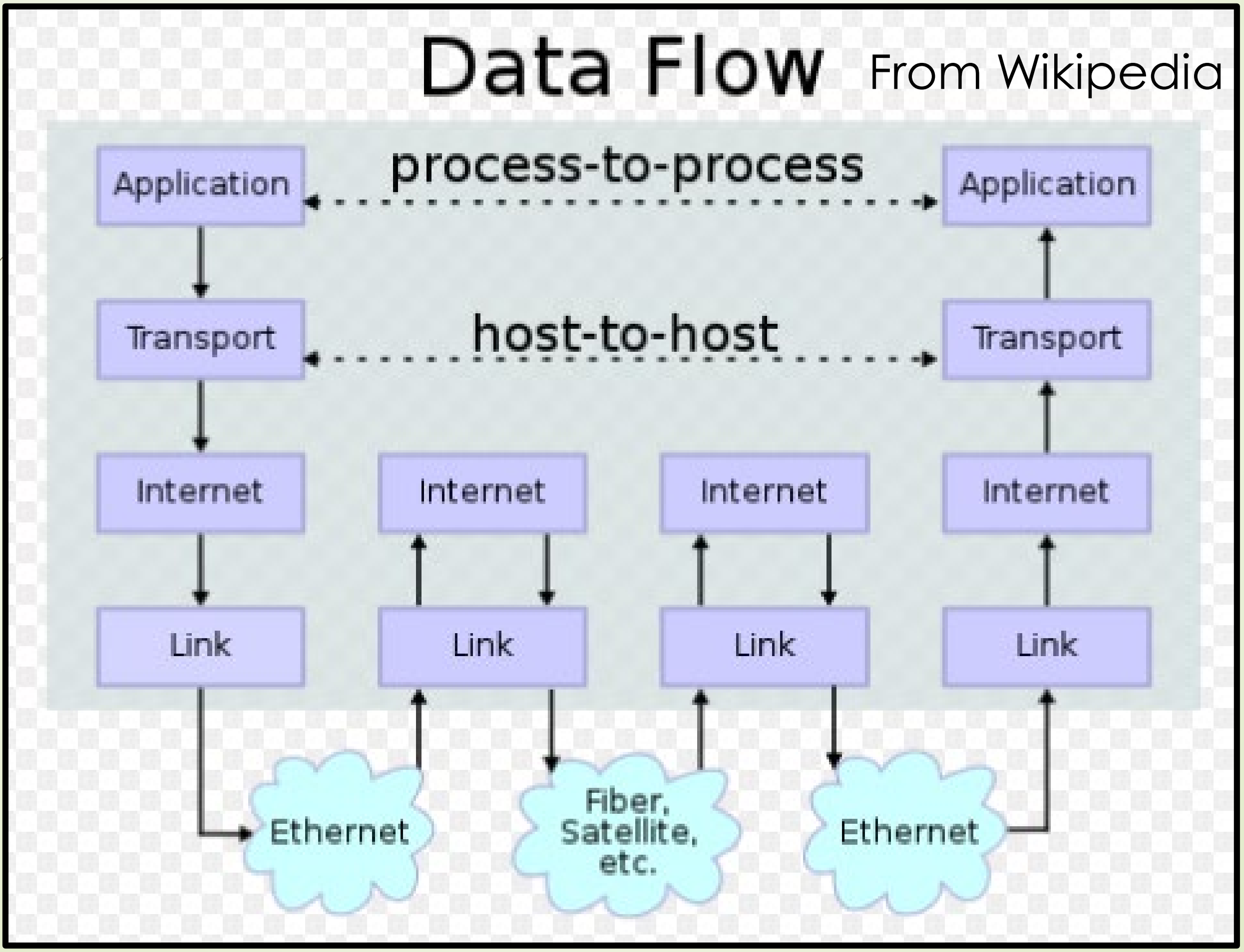
GPT

- Use 64 bits for block address (LBA)
- Max. size of a partition 8ZiB (2^{64} x 512 bytes/block)
- Up to 128 partitions in a physical drive

Evidence in Networks

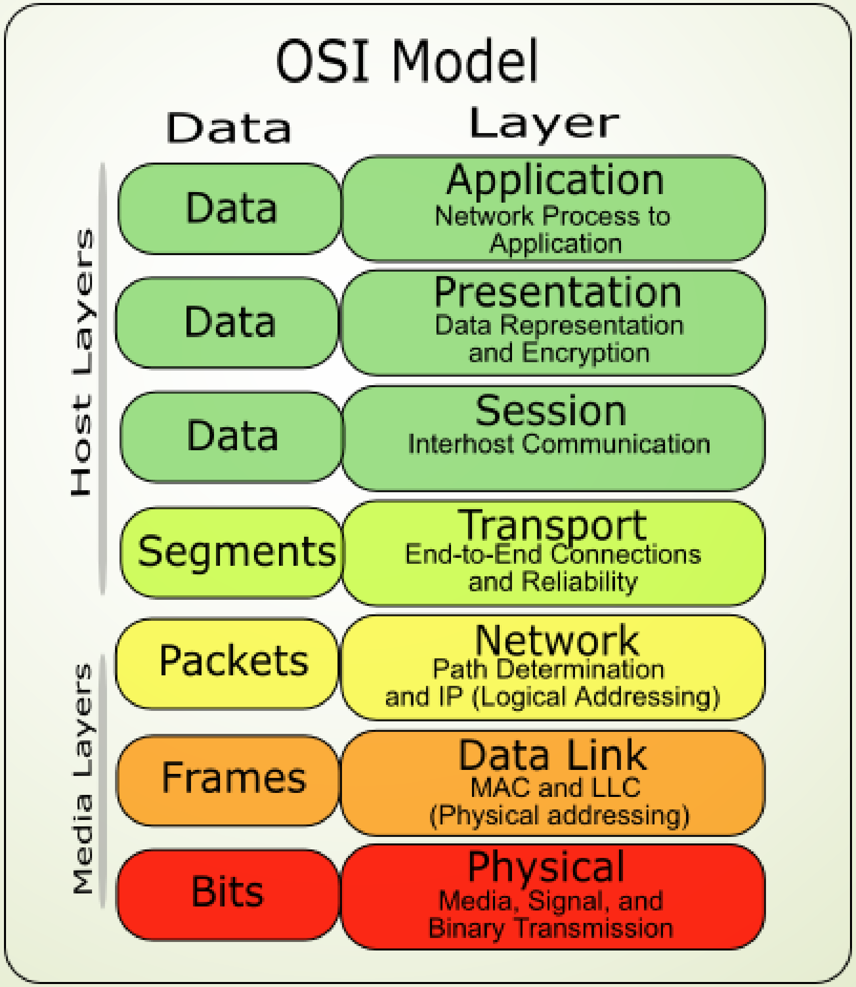
- Network traffic
- Event logs in network devices
  - Routers
  - LAN switches
  - Firewalls
  - Web, Proxy, DNS, Proxy, DNS and Windows Directory domain controllers

Network Traffic – Process-to-Process and Host-to-Host

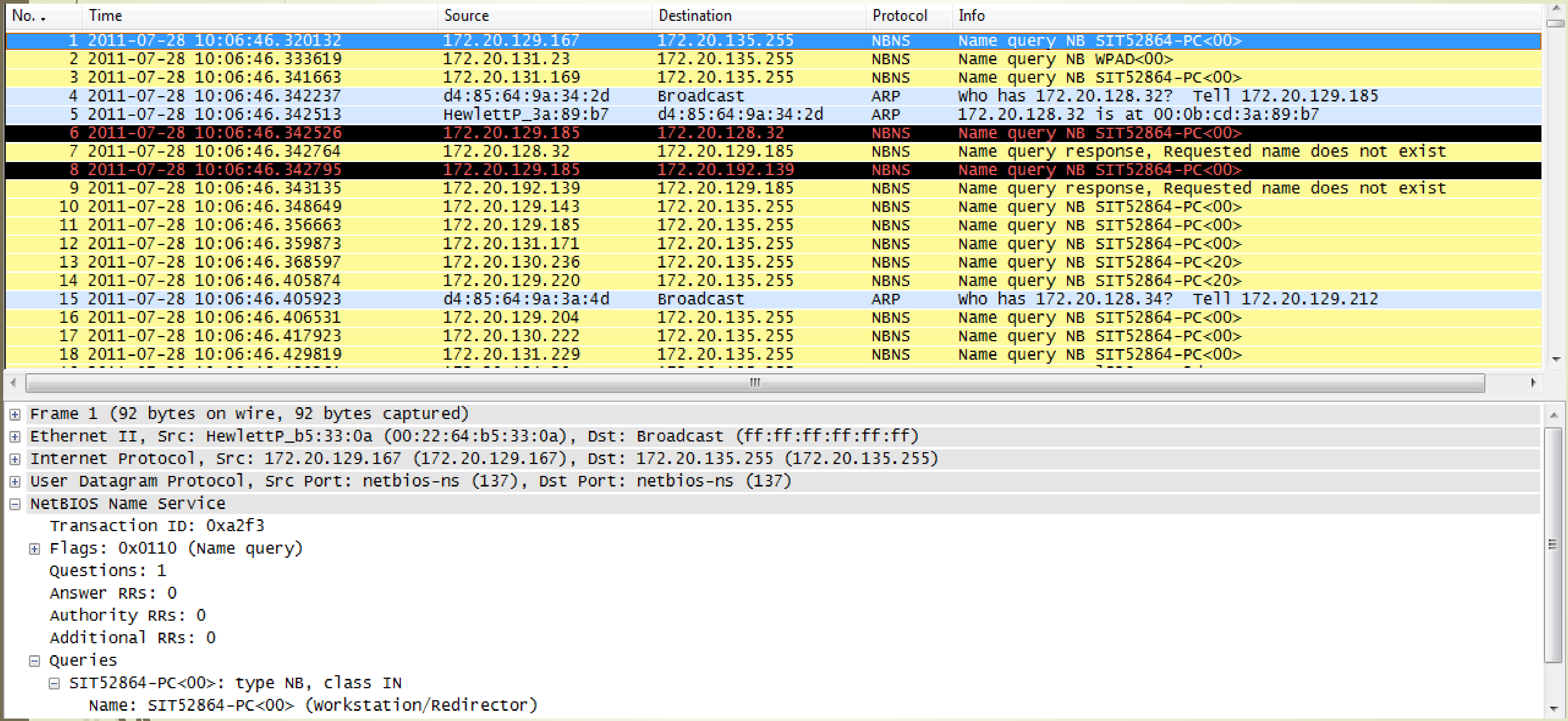


From Wikipedia

Network Traffic – Process-to-Process and Host-to-Host


OSI Model
Data
Layer
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data Representation and Encryption
Data
Session
Interhost Communication
Segments
Transport
End-to-End Connections and Reliability
Packets
Network
Path Determination and IP (Logical Addressing)
Frames
Data Link
MAC and LLC (Physical addressing)
Bits
Physical
Media, Signal, and Binary Transmission

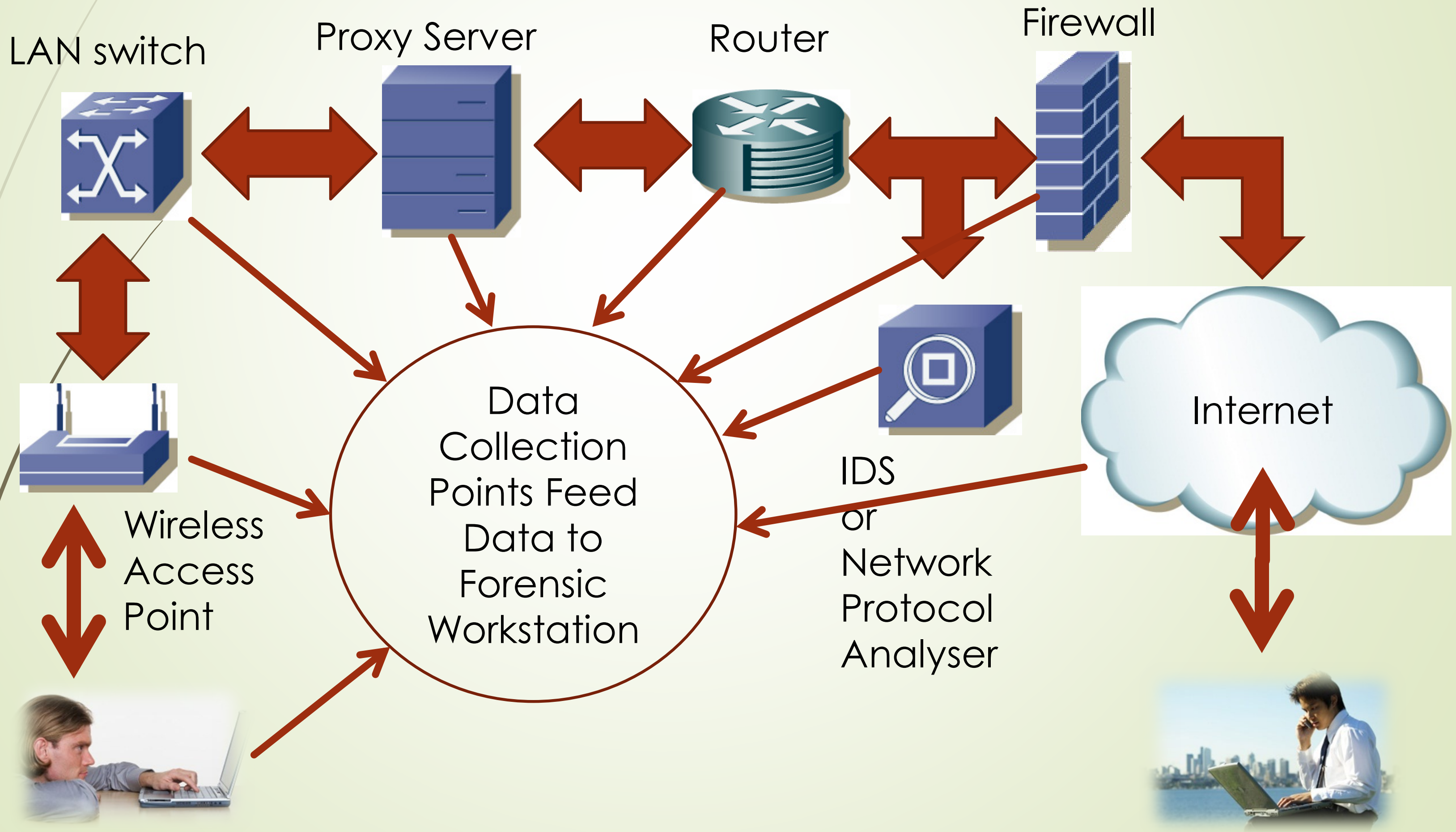
Network Traffic – Process-to-Process and Host-to-Host



No.	Time	Source	Destination	Protocol	Info
1	2011-07-28 10:06:46.320132	172.20.129.167	172.20.135.255	NBNS	Name query NB SIT52864-PC<00>
2	2011-07-28 10:06:46.333619	172.20.131.23	172.20.135.255	NBNS	Name query NB WPAD<00>
3	2011-07-28 10:06:46.341663	172.20.131.169	172.20.135.255	NBNS	Name query NB SIT52864-PC<00>
4	2011-07-28 10:06:46.342237	d4:85:64:9a:34:2d	Broadcast	ARP	Who has 172.20.128.32? Tell 172.20.129.185
5	2011-07-28 10:06:46.342513	HewlettP_3a:89:b7	d4:85:64:9a:34:2d	ARP	172.20.128.32 is at 00:0b:cd:3a:89:b7
6	2011-07-28 10:06:46.342526	172.20.129.185	172.20.128.32	NBNS	Name query NB SIT52864-PC<00>
7	2011-07-28 10:06:46.342764	172.20.128.32	172.20.129.185	NBNS	Name query response, Requested name does not exist
8	2011-07-28 10:06:46.342795	172.20.129.185	172.20.192.139	NBNS	Name query NB SIT52864-PC<00>
9	2011-07-28 10:06:46.343135	172.20.192.139	172.20.129.185	NBNS	Name query response, Requested name does not exist
10	2011-07-28 10:06:46.348649	172.20.129.143	172.20.135.255	NBNS	Name query NB SIT52864-PC<00>
11	2011-07-28 10:06:46.356663	172.20.129.185	172.20.135.255	NBNS	Name query NB SIT52864-PC<00>
12	2011-07-28 10:06:46.359873	172.20.131.171	172.20.135.255	NBNS	Name query NB SIT52864-PC<00>
13	2011-07-28 10:06:46.368597	172.20.130.236	172.20.135.255	NBNS	Name query NB SIT52864-PC<20>
14	2011-07-28 10:06:46.405874	172.20.129.220	172.20.135.255	NBNS	Name query NB SIT52864-PC<20>
15	2011-07-28 10:06:46.405923	d4:85:64:9a:3a:4d	Broadcast	ARP	Who has 172.20.128.34? Tell 172.20.129.212
16	2011-07-28 10:06:46.406531	172.20.129.204	172.20.135.255	NBNS	Name query NB SIT52864-PC<00>
17	2011-07-28 10:06:46.417923	172.20.130.222	172.20.135.255	NBNS	Name query NB SIT52864-PC<00>
18	2011-07-28 10:06:46.429819	172.20.131.229	172.20.135.255	NBNS	Name query NB SIT52864-PC<00>

```
⊞ Frame 1 (92 bytes on wire, 92 bytes captured)
⊞ Ethernet II, Src: HewlettP_b5:33:0a (00:22:64:b5:33:0a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol, Src: 172.20.129.167 (172.20.129.167), Dst: 172.20.135.255 (172.20.135.255)
⊞ User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)
⊟ NetBIOS Name Service
    Transaction ID: 0xa2f3
  ⊞ Flags: 0x0110 (Name query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ SIT52864-PC<00>: type NB, class IN
        Name: SIT52864-PC<00> (Workstation/Redirector)
```

Event logs in network devices


LAN switch
Proxy Server
Router
Firewall
Internet
Wireless Access Point
Data Collection Points Feed Data to Forensic Workstation
IDS or Network Protocol Analyser

Q7: Which of the following network devices can capture network traffic between any external Internet computers and any computers in a company intranet?

a) Internet firewall

b) Intranet router

c) An intranet server

d) Any one of the computers in the intranet

See Answer in the last slide of this lecture note

Q7: Which of the following network devices can capture network traffic between any external Internet computers and any computers in a company intranet?

a) **Internet firewall**

b) Intranet router

c) An intranet server

d) Any one of the computers in the intranet

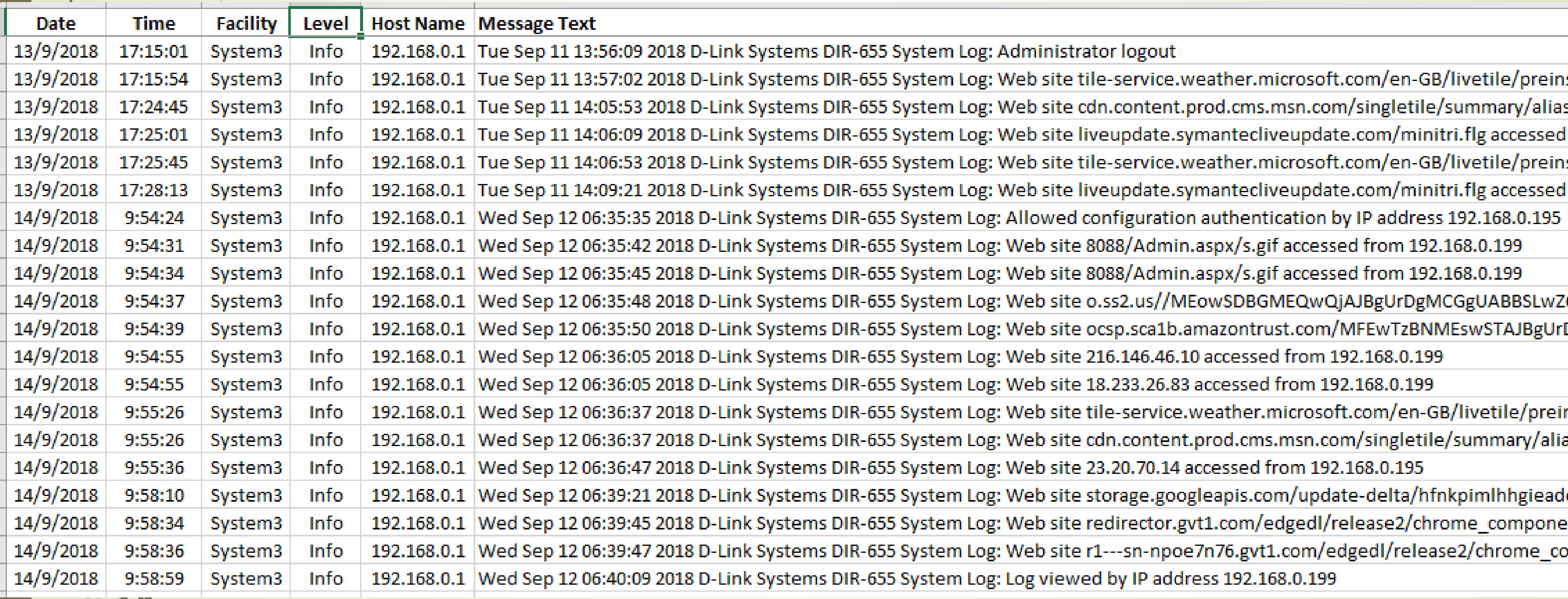
See Answer in the last slide of this lecture note

Further Reading

- Read Section 4 “Using Data from Data Files” and Section 5 “Using Data From Network Traffic” in

Guide to Integrating Forensic Techniques into Incident Response SP 800-86, NIST

A sample syslog events collected from D-Link router 192.168.0.1



Date	Time	Facility	Level	Host Name	Message Text
13/9/2018	17:15:01	System3	Info	192.168.0.1	Tue Sep 11 13:56:09 2018 D-Link Systems DIR-655 System Log: Administrator logout
13/9/2018	17:15:54	System3	Info	192.168.0.1	Tue Sep 11 13:57:02 2018 D-Link Systems DIR-655 System Log: Web site tile-service.weather.microsoft.com/en-GB/livetile/prein
13/9/2018	17:24:45	System3	Info	192.168.0.1	Tue Sep 11 14:05:53 2018 D-Link Systems DIR-655 System Log: Web site cdn.content.prod.cms.msn.com/singletile/summary/alias
13/9/2018	17:25:01	System3	Info	192.168.0.1	Tue Sep 11 14:06:09 2018 D-Link Systems DIR-655 System Log: Web site liveupdate.symantecliveupdate.com/minitri.flg accessed
13/9/2018	17:25:45	System3	Info	192.168.0.1	Tue Sep 11 14:06:53 2018 D-Link Systems DIR-655 System Log: Web site tile-service.weather.microsoft.com/en-GB/livetile/prein
13/9/2018	17:28:13	System3	Info	192.168.0.1	Tue Sep 11 14:09:21 2018 D-Link Systems DIR-655 System Log: Web site liveupdate.symantecliveupdate.com/minitri.flg accessed
14/9/2018	9:54:24	System3	Info	192.168.0.1	Wed Sep 12 06:35:35 2018 D-Link Systems DIR-655 System Log: Allowed configuration authentication by IP address 192.168.0.195
14/9/2018	9:54:31	System3	Info	192.168.0.1	Wed Sep 12 06:35:42 2018 D-Link Systems DIR-655 System Log: Web site 8088/Admin.aspx/s.gif accessed from 192.168.0.199
14/9/2018	9:54:34	System3	Info	192.168.0.1	Wed Sep 12 06:35:45 2018 D-Link Systems DIR-655 System Log: Web site 8088/Admin.aspx/s.gif accessed from 192.168.0.199
14/9/2018	9:54:37	System3	Info	192.168.0.1	Wed Sep 12 06:35:48 2018 D-Link Systems DIR-655 System Log: Web site o.ss2.us//MEowSDBGMEQwQjAJBgUrDgMCGgUABBSLwZ
14/9/2018	9:54:39	System3	Info	192.168.0.1	Wed Sep 12 06:35:50 2018 D-Link Systems DIR-655 System Log: Web site ocsp.sca1b.amazontrust.com/MFEwTzBNMEswSTAJBgUrD
14/9/2018	9:54:55	System3	Info	192.168.0.1	Wed Sep 12 06:36:05 2018 D-Link Systems DIR-655 System Log: Web site 216.146.46.10 accessed from 192.168.0.199
14/9/2018	9:54:55	System3	Info	192.168.0.1	Wed Sep 12 06:36:05 2018 D-Link Systems DIR-655 System Log: Web site 18.233.26.83 accessed from 192.168.0.199
14/9/2018	9:55:26	System3	Info	192.168.0.1	Wed Sep 12 06:36:37 2018 D-Link Systems DIR-655 System Log: Web site tile-service.weather.microsoft.com/en-GB/livetile/prein
14/9/2018	9:55:26	System3	Info	192.168.0.1	Wed Sep 12 06:36:37 2018 D-Link Systems DIR-655 System Log: Web site cdn.content.prod.cms.msn.com/singletile/summary/alia
14/9/2018	9:55:36	System3	Info	192.168.0.1	Wed Sep 12 06:36:47 2018 D-Link Systems DIR-655 System Log: Web site 23.20.70.14 accessed from 192.168.0.195
14/9/2018	9:58:10	System3	Info	192.168.0.1	Wed Sep 12 06:39:21 2018 D-Link Systems DIR-655 System Log: Web site storage.googleapis.com/update-delta/hfnkpimlhhgiead
14/9/2018	9:58:34	System3	Info	192.168.0.1	Wed Sep 12 06:39:45 2018 D-Link Systems DIR-655 System Log: Web site redirector.gvt1.com/edgedl/release2/chrome_compone
14/9/2018	9:58:36	System3	Info	192.168.0.1	Wed Sep 12 06:39:47 2018 D-Link Systems DIR-655 System Log: Web site r1---sn-npoe7n76.gvt1.com/edgedl/release2/chrome_co
14/9/2018	9:58:59	System3	Info	192.168.0.1	Wed Sep 12 06:40:09 2018 D-Link Systems DIR-655 System Log: Log viewed by IP address 192.168.0.199

Summary

- You are able to list the evidence items in computers and networks
- Evidence in computers is in file systems, operating systems, applications and computer memory
- One or more File systems are hosted in a physical disk drives with different interfaces connecting to a computer
- Files are stored in sectors of a partition in a physical disk drive
- RAID 0, 1 and 5 provide different levels of redundancy
- Evidence in networks is in network traffic and network devices event logs

Answers to questions in this lecture note

- Q1 : b
- Q2 : d
- Q3 : d
- Q4 : c
- Q5 : c
- Q6 : b
- Q7 : a