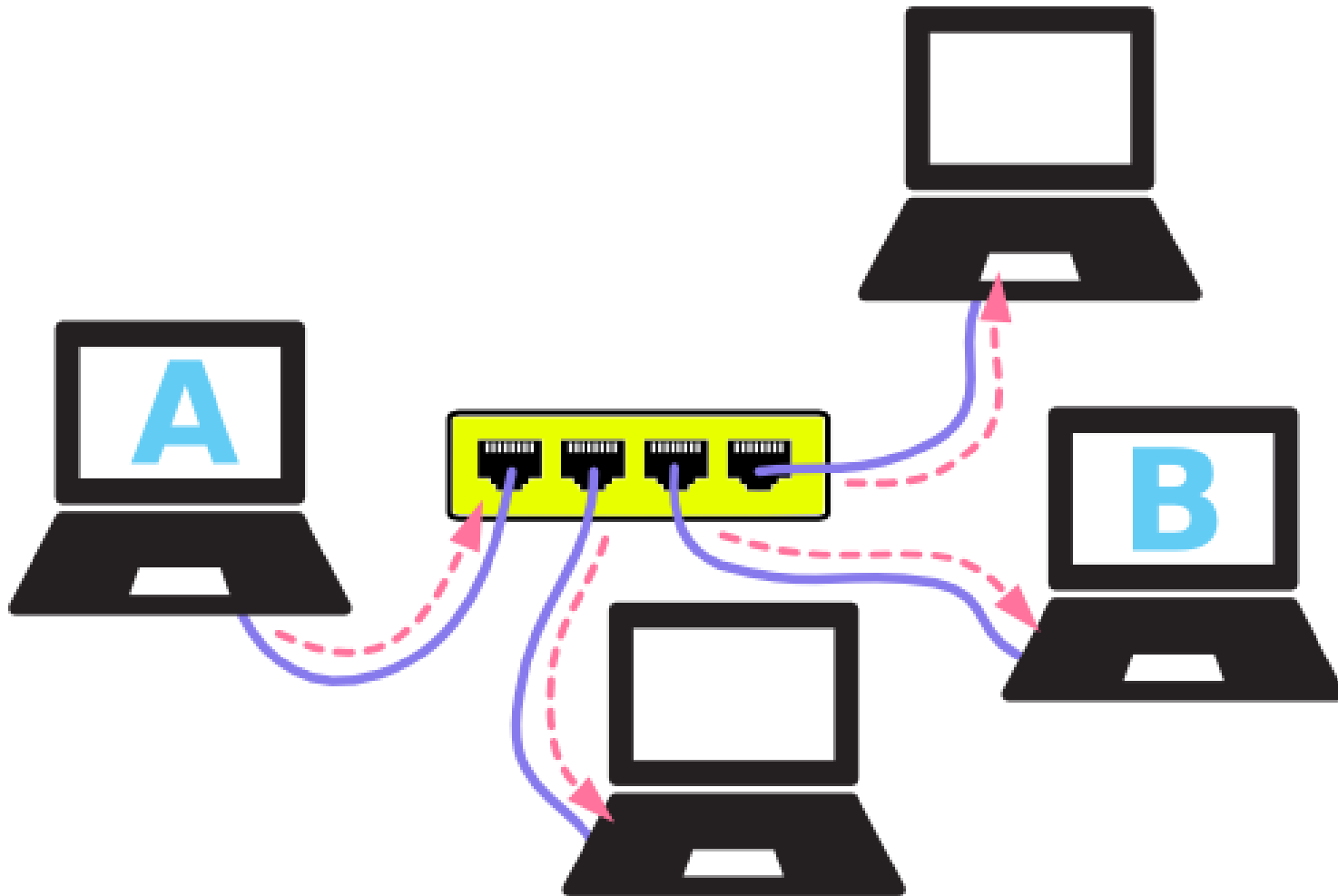


# Network Concepts

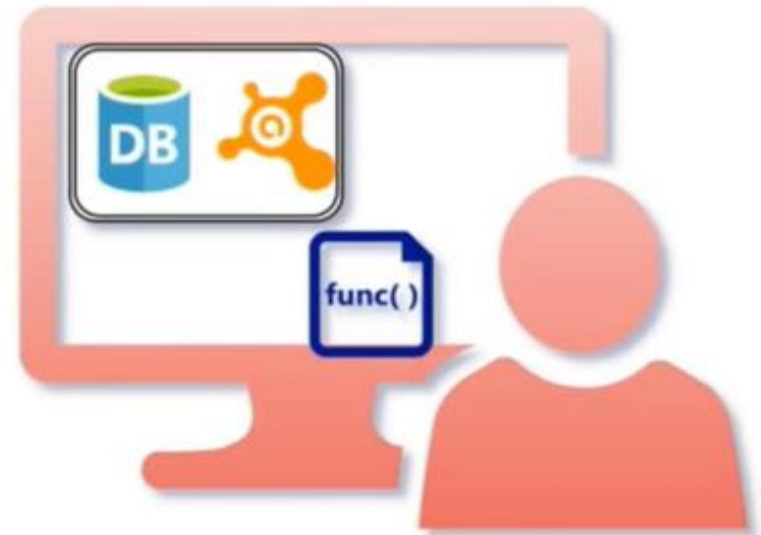


# Network Security Devices

- Antivirus
- IDS/IPS
- Firewall

# Antivirus

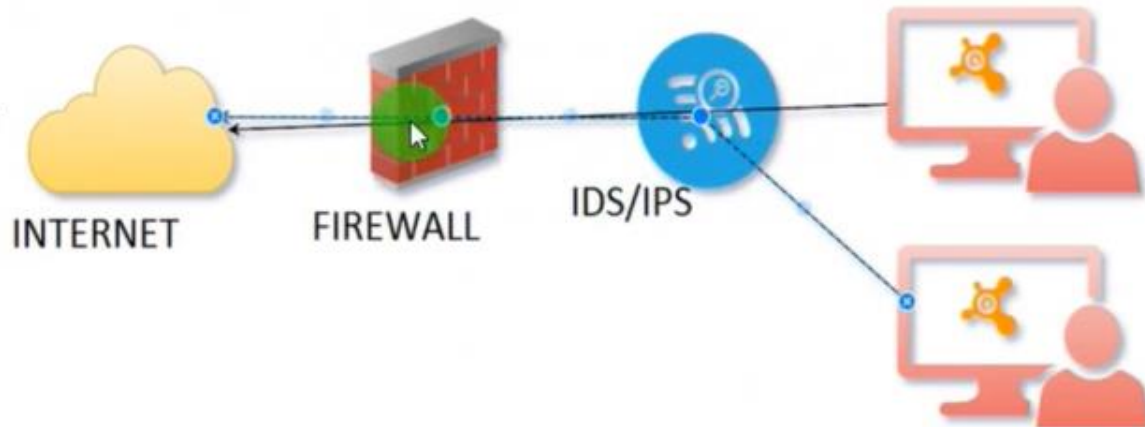
- ▶ Antivirus will scan the file.
- ▶ Check the content of payload in the file and try to match with the signature exist in the database
- ▶ If match exist, it will take action or clean/delete the file.
- ▶ Otherwise, it will mark it as a safe.





# IDS/IPS?

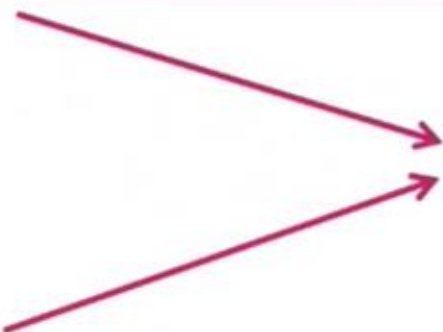
- ▶ IDS stands for Intrusion Detection System for alerting on the attack.
- ▶ IPS stands for Intrusion Prevention System for alerting and blocking the attack.
- ▶ IDS/IPS consist of signature, it match the content of the packet with the signature and take the action accordingly.



# Computer Network

## IDS Signature

```
13 March 2018 05:32:21.11 TCP Any Any -> 192.154.31.1 80 content:"  
image?id=1OACCYOE0-eoTRTfsB " msg: "SQL injection detected"
```



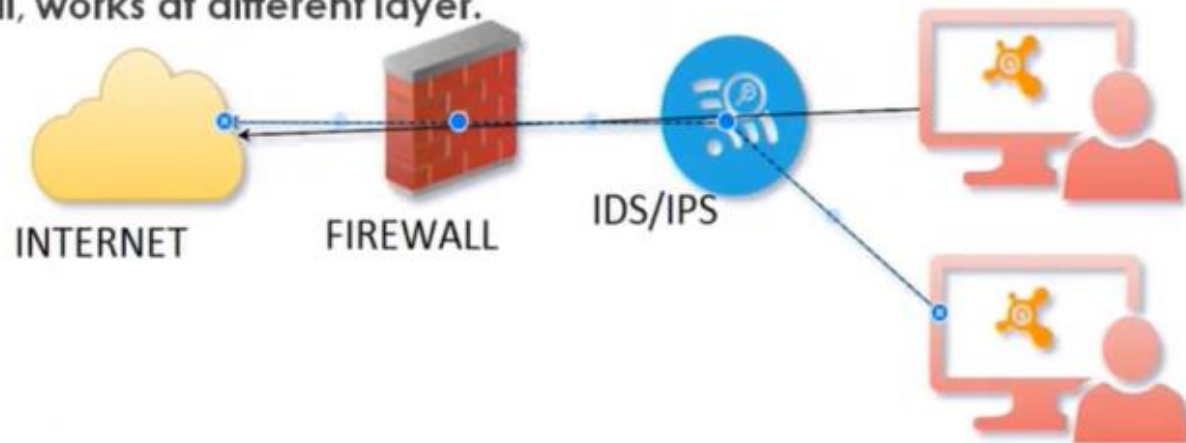
**MATCH Successful**

```
GET /image?id=1OACCYOE0-eoTRTfsB...X1NMN9nz599ufI1Jh0CggPFA_sK80AGkIr8pLTYRpNUKPMwtEa&options=w1600 HTTP/1.1  
Host: themes.googleusercontent.com  
User-Agent: Mozilla/5.0 (Windows NT 6.2; Win64; x64; rv:60.0) Gecko/20100101 Firefox/60.0  
Accept: /*/*  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Referer: http://www.bitumenwasher.com/  
Connection: Keep-Alive
```

**Network Packet**

# Firewall

- ▶ The basic functionality of Firewall to allowed or blocked the traffic on the basis of Source IP, Destination IP, Source Port and Destination Port.
- ▶ There are different type of firewall, works at different layer.
- ▶ Types of Firewall
  1. Packet level Firewall
  2. State full Inspection Firewall
  3. Application level Firewall



Source IP	Source Port	Destination	Destination Port	Action
192.15.1.1	any	Any	80	Allow
any	any	12.13.12.1	any	Block
any	any	124.123.12.1	any	Block

# Packet Understanding

## Bit, Hexadecimal & Bytes Representation

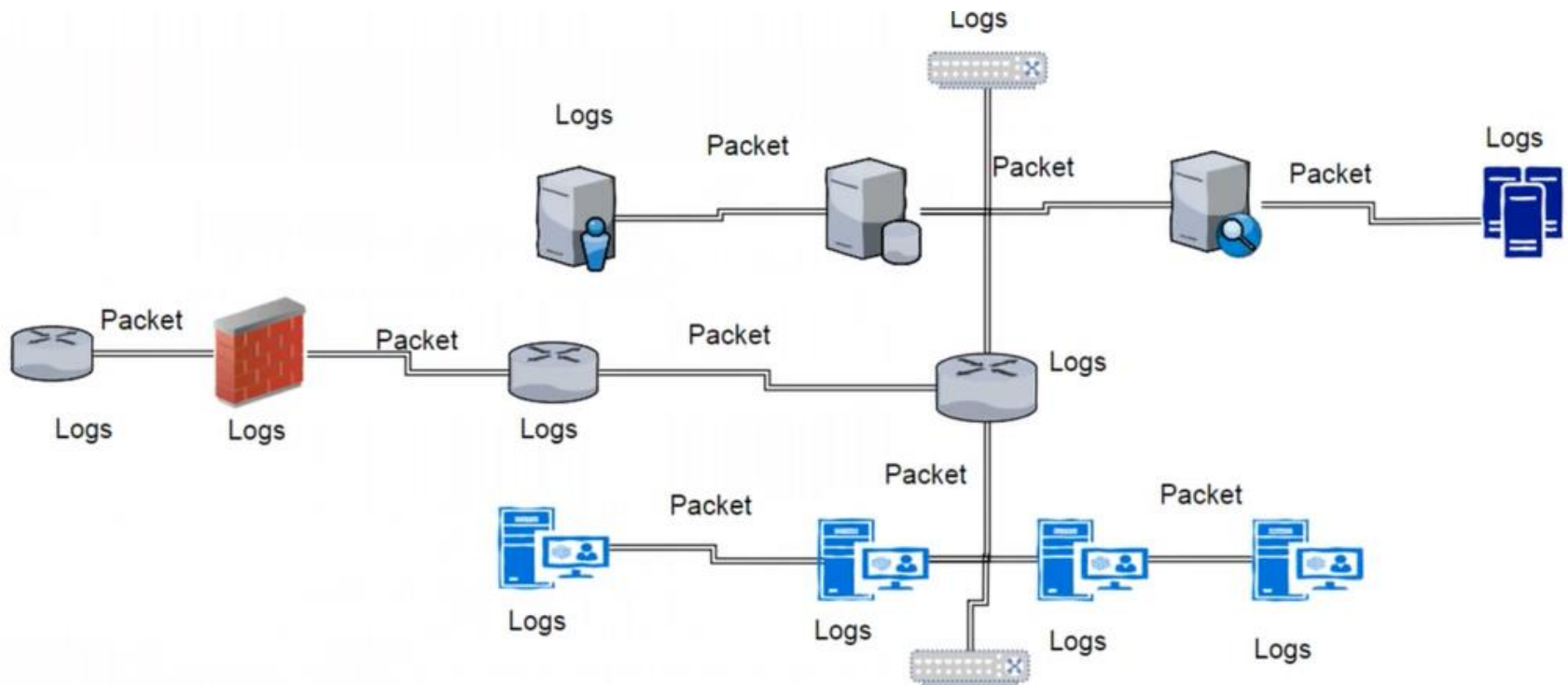
# Packet vs Log

▶ Security breach Identification and Investigation is based on two sources.

1. Network Packets
2. Device log

➤ Network Packet : Packet is collection of data that can be used by computers which need to communicate with each other

➤ Device log : A file that lists actions that have occurred. For example, Web servers maintain log files listing every request made to the server



# Network Packet Capture

No.	Time	Source	Destination	Prot	Length	Info
32	324487	2.132.236.194	192.168.1.111	UDP	160	49698 → 12570 Len=118

## Summary

```
▶ Frame 78: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface 0
▶ Ethernet II, Src: D-LinkIn_80:d1:dc (a0:ab:1b:80:d1:dc), Dst: Shenzhen_a2:f5:e8 (28:f3:66:a2:f5:e8)
▶ Internet Protocol Version 4, Src: 2.132.236.194, Dst: 192.168.1.111
▶ User Datagram Protocol, Src Port: 49698 (49698), Dst Port: 12570 (12570)
▶ Data (118 bytes)
  Data: 64313a6164323a696432303a4a13d51caf8baaaa47bcd085...
  [Length: 118]
```

## Decoded Information

```
0000 28 f3 66 a2 f5 e8 a0 ab 1b 80 d1 dc 08 00 45 00 (.f.....E.
0010 00 92 73 4d 00 00 33 11 62 b0 02 84 ec c2 c0 a8 ..sM..3. b.....
0020 01 6f c2 22 31 1a 00 7e 47 29 64 31 3a 61 64 32 .o."1..~ G)d1:ad2
0030 3a 69 64 32 30 3a 4a 13 d5 1c af 8b aa aa 47 bc :id20:J. ....G.
0040 d0 85 c8 1d 2e dd dd 05 ac 15 36 3a 74 61 72 67 ..... ..6:targ
0050 65 74 32 30 3a 4a 13 d5 1c af 8b aa aa 47 bc d0 et20:J.. ....G..
0060 85 c8 1d 2e dd dd 05 ac 15 34 3a 77 61 6e 74 6c ..... .4:wantl
0070 32 3a 6e 34 32 3a 6e 36 65 65 31 3a 71 39 3a 66 2:n42:n6 ee1:q9:f
0080 69 6e 64 5f 6e 6f 64 65 31 3a 74 32 3a f0 36 31 ind_node 1:t2:.61
0090 3a 76 35 3a 41 7a 07 d0 a1 31 3a 79 31 3a 71 65 :v5:Az.. .1:y1:qe
```

## Raw packet

# Computer Network

## Network Packet

```
0000 28 f3 66 a2 f5 e8 a0 ab 1b 80 d1 dc 08 00 45 00 (.f.....E.
0010 00 81 00 00 40 00 3b 11 52 5a 02 31 28 ca c0 a8 ....@.;. RZ.1(...
0020 01 6f 11 3c 31 1a 00 6d 23 6a 64 31 3a 61 64 32 .o.<1.m #jd1:ad2
0030 3a 69 64 32 30 3a 4a 11 1e 0e a9 5e c8 c6 1e 37 :id20:J. ...^...7
0040 da 59 7b 15 e0 25 e3 e3 49 04 36 3a 74 61 72 67 .Y{..%.. I.6:targ
0050 65 74 32 30 3a 4a 13 b2 65 55 53 c6 3f 99 04 d4 et20:J.. eUS.?...
0060 53 0a d9 d9 24 d0 3e 21 b7 65 31 3a 71 39 3a 66 S...$.>! .e1:q9:f
0070 69 6e 64 5f 6e 6f 64 65 31 3a 74 32 3a 38 d6 31 ind_node 1:t:8.1
0080 3a 76 34 3a 4c 54 00 10 31 3a 79 31 3a 71 65 :v4:LT.. 1:y1:qe
```

## Device Logs

General Details

Credential Manager credentials were read.

Subject:

Security ID:	SYSTEM
Account Name:	DESKTOP-79N14PKS
Account Domain:	WORKGROUP
Logon ID:	0x3E7
Read Operation:	Enumerate Credentials

This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	7/29/2021 7:00:32 AM
Event ID:	5379	Task Category:	User Account Management
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DESKTOP-79N14PK
OpCode:	Info		
More Information:	<a href="#">Event Log Online Help</a>		

# Encoding and Decoding:

Encoding is the process of putting a sequence of characters such as letters, numbers, and other special characters into a specialized format for efficient transmission.

Decoding is the process of converting an encoded format back into the original sequence of characters.

It is completely different from Encryption which we usually misinterpret. Encoding and decoding are used in data communications and storage.

Encoding should NOT be used for transporting sensitive information.

# Encryption

Encryption is the process of translating plain text data ([plaintext](#)) into something that appears to be random and meaningless ([ciphertext](#)).

Decryption is the process of converting ciphertext back to plaintext.

## Types of Encryption:

There are two types of encryption in widespread use **symmetric** and **asymmetric** encryption.

# What is symmetric encryption?

In symmetric encryption the same key is used for encryption and decryption.

It is therefore critical that a secure method is considered to transfer the key between sender and recipient.

Symmetric encryption – Using the same key for encryption and decryption.

# What is asymmetric encryption?

Asymmetric encryption uses the notion of a key pair: a different key is used for the encryption and decryption process.

One of the keys is typically known as the private key and the other is known as the public key.

The private key is kept secret by the owner and the public key is either shared amongst authorised recipients or made available to the public at large.

Data encrypted with the recipient's public key can only be decrypted with the corresponding private key.

Data can therefore be transferred without the risk of unauthorised or unlawful access to the data. Asymmetric encryption – Using a different key for the encryption and decryption process.

# Thanks