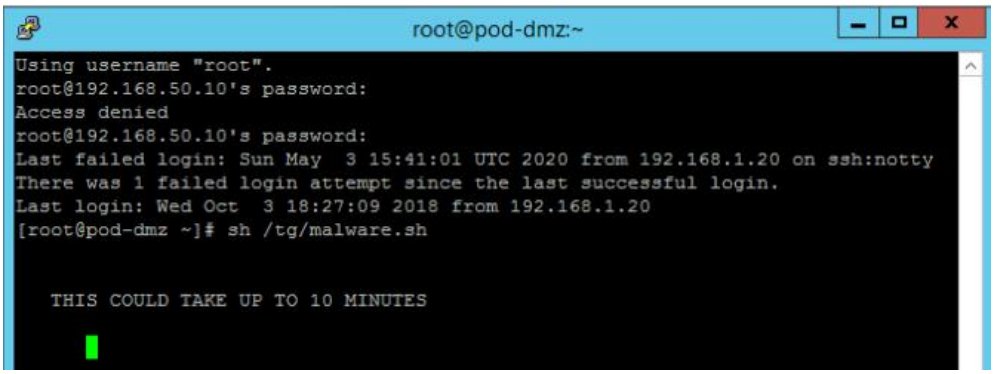
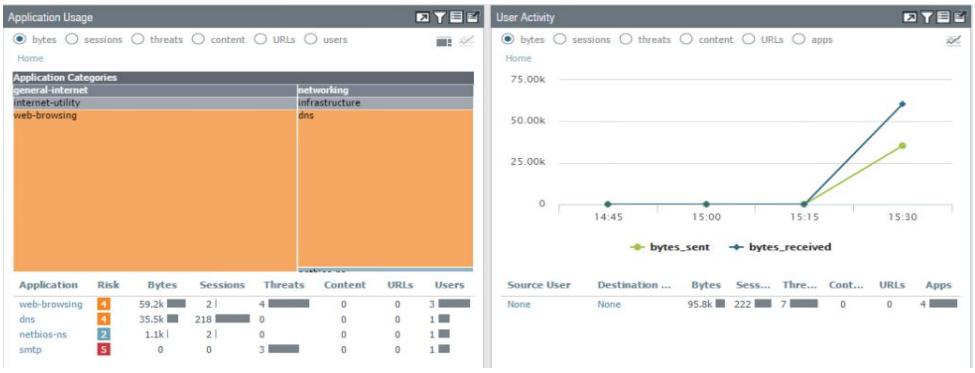
SIDDHANT GAHTORI
GATEWAY PROJECT 2

Module 1A (LAB 6): Using the Application Command Center

Summary: In this module, firstly we generated malware traffic towards firewall. Then to analyze the threat activity we clicked on Threat Activity tab on ACC Menu. After that we can see the network surge and unwanted activity on the firewall end.



- Sending the malware traffic to firewall.



- Network Surge during the activity

- Threat Activity Monitor

Module 1B (LAB 7): Analyzing Firewall Logs

Summary: In this module, firstly we generated malware traffic towards firewall. Then to analyze the logs we clicked on Monitor tab on Menu. After that we can see and analyze every kind of traffic.

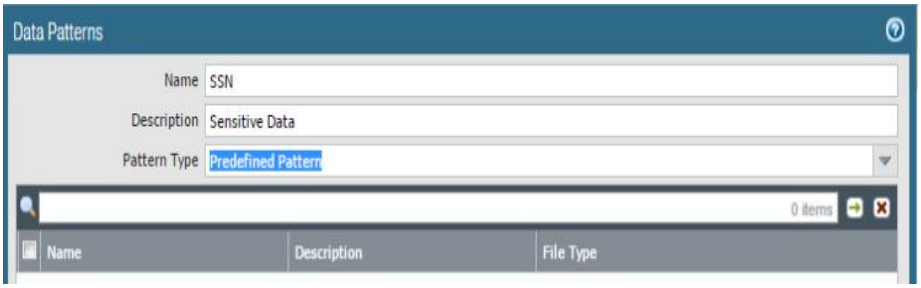
(app eq web-browsing)

Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port
05/03 16:24:33	end	inside	outside	192.168.1.20		172.217.129.38	80
05/03 16:24:33	end	inside	outside	192.168.1.20		173.194.162....	80
05/03 16:24:33	end	inside	outside	192.168.1.20		216.58.192.238	80
05/19 23:26:58	end	inside	outside	192.168.1.20		204.79.197.200	80
05/19 22:03:06	end	inside	outside	192.168.1.20		74.125.155.251	80
05/19 22:03:06	end	inside	outside	192.168.1.20		172.217.15.110	80

- Analyzing traffic for web based activities

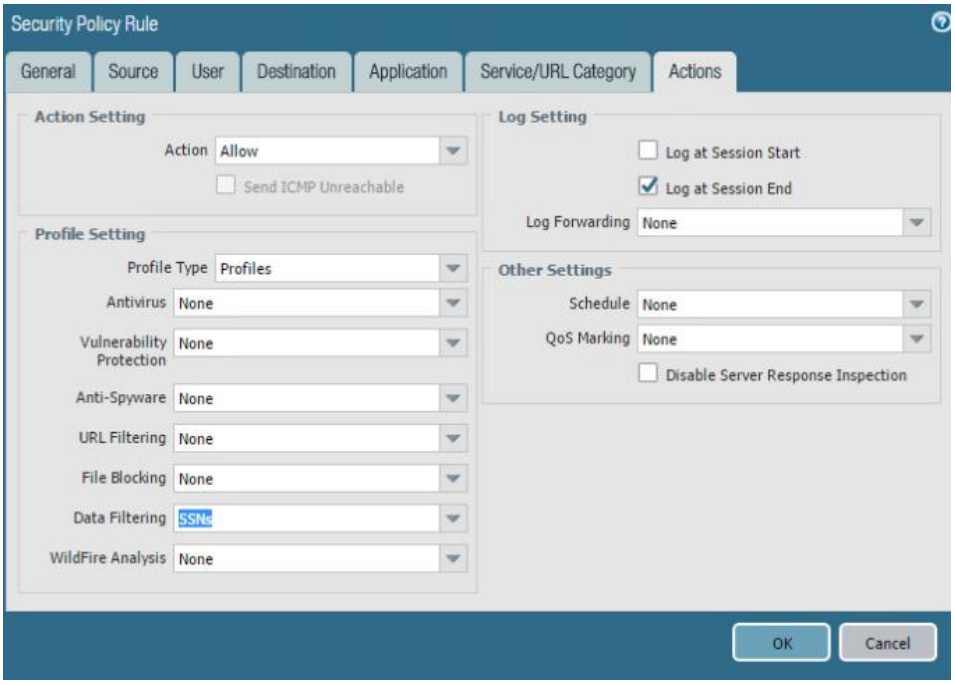
Module 2A (LAB 8): Protecting Sensitive Data

Summary: In this module first we made a policy to restrict access of certain type of traffic for a predefined pattern. After that we tested and verified that policy. We monitored sensitive data like social security numbers in palo alto networks firewall.

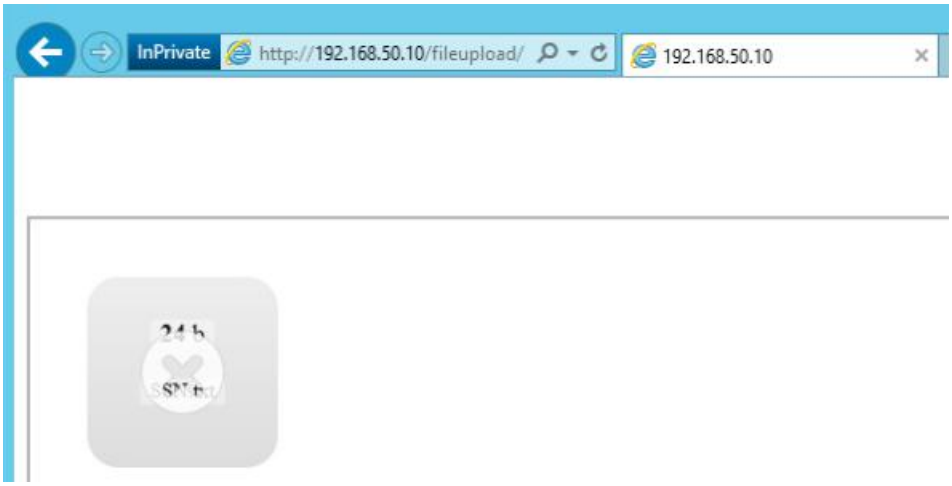


- Defining Data Patterns

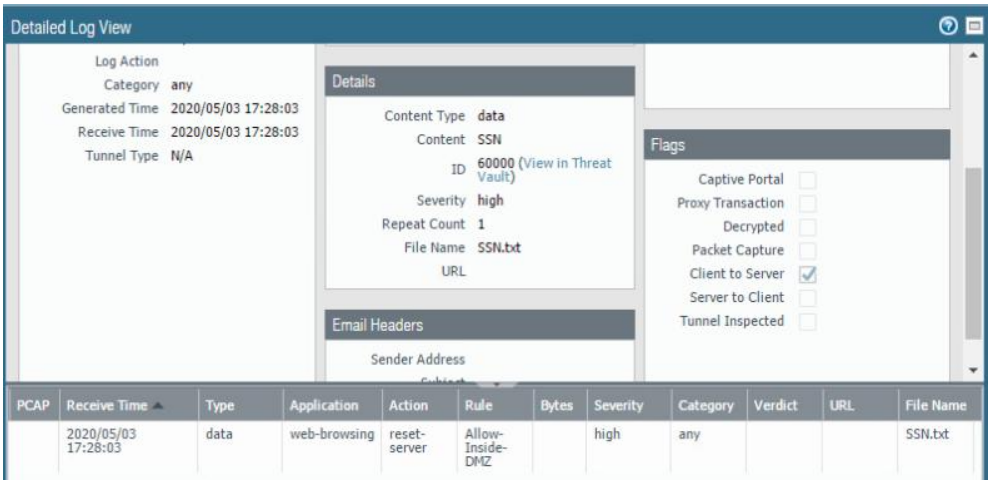
- Defining Data Filtering Profile for Social Security Numbers



- Creating firewall rules



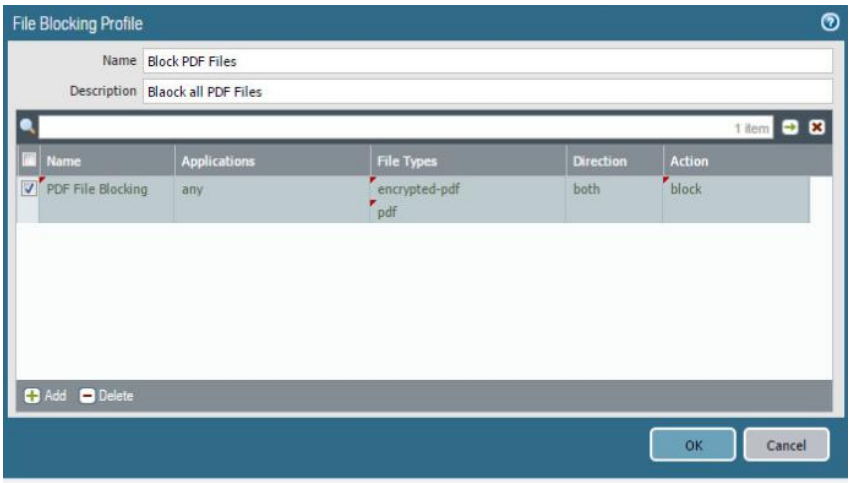
◆ Testing the Policy



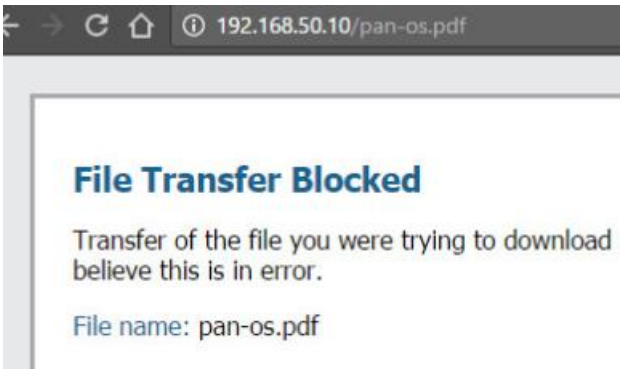
◆ Verifying the Policy

Module 2B (LAB 9): File Blocking

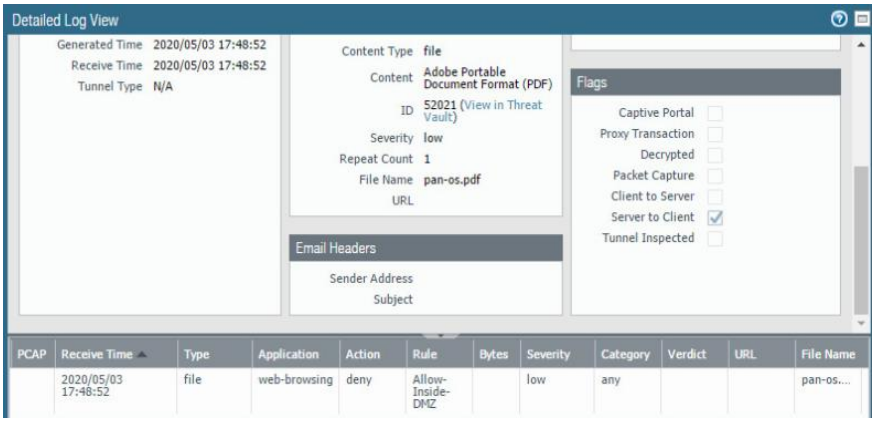
Summary: Objectives of this module consist of creating, applying and testing File Blocking Security Profile. To achieve that, first we clicked File Blocking option from Object Tab. After that we made a policy to block all kind of PDF Files and added to the firewall rules. Then we tested the rule and analyzed the logs.



- Creation of File Blocking Rule for PDF Files



- Testing of the Rule

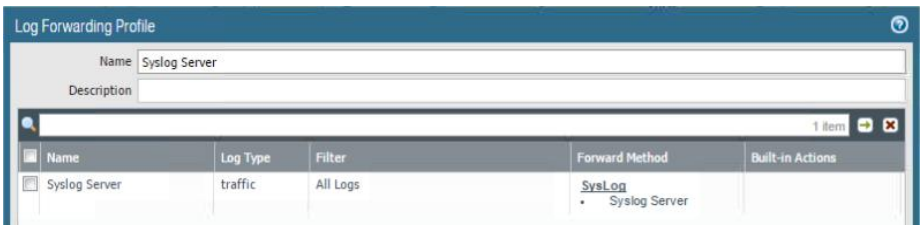


- Log Analysis of Unwanted Action

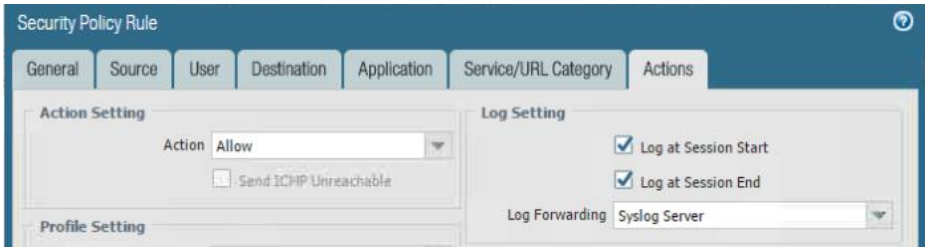
Module 3A (LAB 10): Log Forwarding

Summary: In this module, the objective is to configure Syslog on palo alto firewall and verify Syslog forwarding. For that, A First we clicked Device > Syslog tab. Then we add a Syslog server at IP of 192.168.50.10. Then we clicked Objects > Log Forwarding option. Then in Log Settings, we added Syslog Server. Then we changed security policy to modify log forwarding option. Then we verified the implementation.

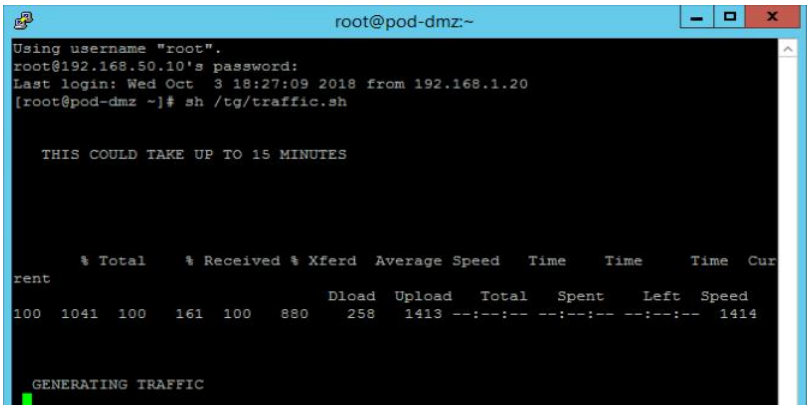
- Syslog Server Profile Configurations



- Creating Log Forwarding Profile



- Security Policy Rule Configurations



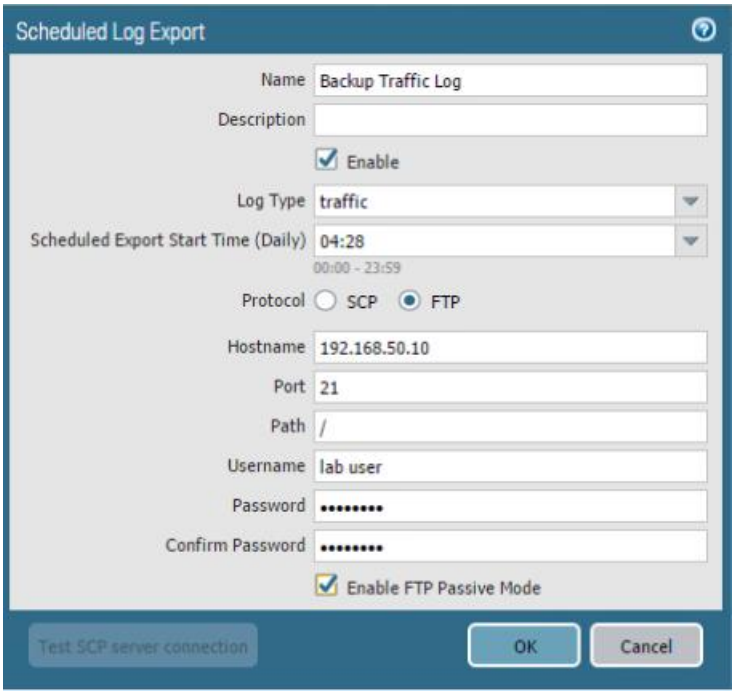
- Traffic Generation

```
root@pod-dmz:~
FFIC,start,1,2020/05/04 02:19:38,192.168.1.20,192.168.50.10,0.0.0.0,0.0.0.0,Allo
w-Any,,,dns,vsys1,inside,dmz,ethernet1/2,ethernet1/3,Syslog Server,2020/05/04 02
:19:38,757,1,49913,53,0,0,0x0,udp,allow,90,90,0,1,2020/05/04 02:19:38,0,any,0,28
71,0x0,192.168.0.0-192.168.255.255,192.168.0.0-192.168.255.255,0,1,0,n/a,0,0,0,0
,,lab-firewall,from-policy,,,0,,0,,N/A
May  4 02:19:38 lab-firewall.lab.local 1,2020/05/04 02:19:38,015351000028085,TRA
FFIC,start,1,2020/05/04 02:19:38,192.168.1.20,8.8.8.8,203.0.113.20,8.8.8.8,Allow
-Any,,,dns,vsys1,inside,outside,ethernet1/2,ethernet1/1,Syslog Server,2020/05/04
 02:19:38,758,1,49913,53,10538,53,0x400000,udp,allow,79,79,0,1,2020/05/04 02:19:
38,0,any,0,2872,0x0,192.168.0.0-192.168.255.255,United States,0,1,0,n/a,0,0,0,0,
,lab-firewall,from-policy,,,0,,0,,N/A
May  4 02:19:38 lab-firewall.lab.local 1,2020/05/04 02:19:38,015351000028085,TRA
FFIC,end,1,2020/05/04 02:19:38,192.168.1.20,8.8.8.8,203.0.113.20,8.8.8.8,Allow-A
ny,,,dns,vsys1,inside,outside,ethernet1/2,ethernet1/1,Syslog Server,2020/05/04 0
2:19:38,734,1,65304,53,7250,53,0x400064,udp,allow,184,78,106,2,2020/05/04 02:19:
08,0,any,0,2873,0x0,192.168.0.0-192.168.255.255,United States,0,1,1,aged-out,0,0
,0,0,,lab-firewall,from-policy,,,0,,0,,N/A
```

- Captured Logs & Analysis

Module 3B (LAB 11): Backup Firewall Logs

Summary: In this lab, the objective is to backup firewall logs. At First we go to Schedule Log Export option. We configure settings as per our convenience . After committing the changes, we can go to Monitor > Logs > System to see the backed up logs.



- Log Schedule Setting

- Backed up Logs

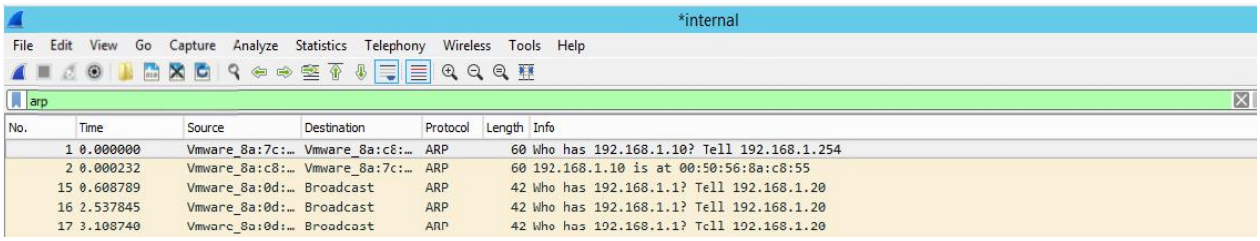
Project Introduction:

In this project, you will utilize Wireshark to initiate a packet capture. Wireshark captures packets and allows network administrators to examine the data within the packet.

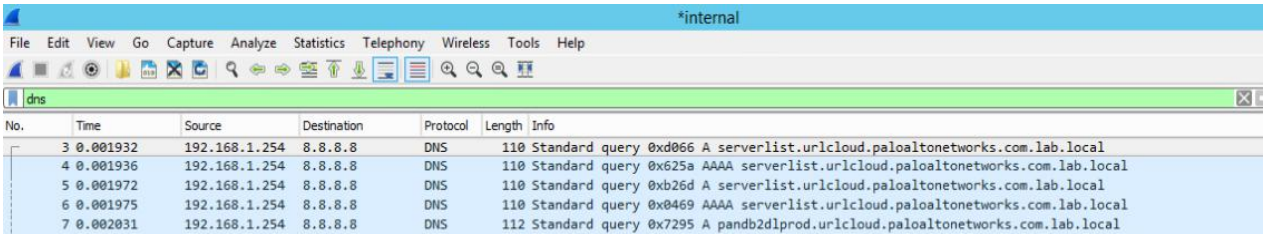
Objective In this project, you will perform the following tasks:

- Create and analyze a Packet Capture using Wireshark

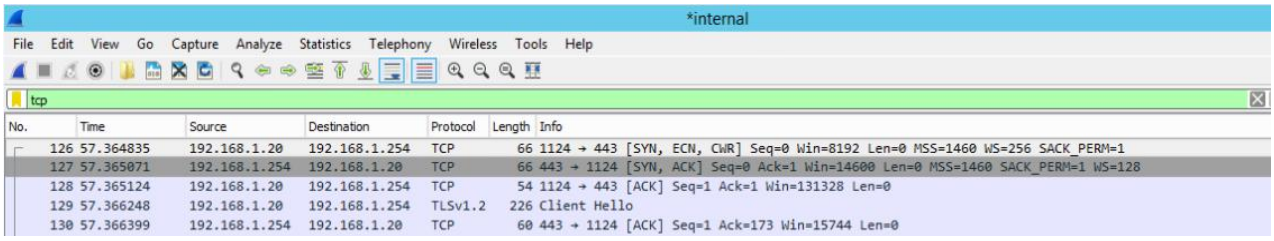
Screenshot:



- ARP Packet Capture



- DNS Captures



- TCP Captures

Wireshark · Packet 1596 · Wi-Fi

```
> Frame 1596: 168 bytes on wire (1344 bits), 168 bytes captured (1344 bits) on interface 0
> Ethernet II, Src: Azurewav_93:2c:81 (80:a5:89:93:2c:81), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 192.168.1.7, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 55536, Dst Port: 1900
v Simple Service Discovery Protocol
  > M-SEARCH * HTTP/1.1\r\n
    HOST: 239.255.255.250:1900\r\n
    MAN: "ssdp:discover"\r\n
    MX: 1\r\n
    ST: urn:dial-multiscreen-org:service:dial:1\r\n
    \r\n
    [Full request URI: http://239.255.255.250:1900*]
    [HTTP request 1/1]
```

◆ HTTP Captures

<u>Explanations:</u>

1. **Function of ARP : Conversion between IP and MAC Addresses**
2. **Purpose of DNS : Converting IP Addresses to Domain Names on Port 53**
3. **Working of TCP : 3 way handshake (SYN, SYN-ACK, ACK) Packets**
4. **Purpose of HTTP : Web Based Communications on Port 80**

----------THE_END----------