**Protocol Analysis Experiment #1**

**Protocols : HTTP, DNS & TCP**

**Application Scenario**

Client requests a file from a server

Server returns the file

Nature of the file : html : Simple one line text

**Protocols to be analysed**

Analyse how protocols DNS, HTTP & TCP are used in running this application. Analysis to be done in 3 parts

**Part#1 : DNS**

**Part #2 : HTTP**

**Part #3 : TCP**

**Trace File to be analysed : HTTP-Tracefiles\http-trace-1 Part#1 : Protocol - DNS**

Client

Server

DNS

-

Request

DNS

-

Reply

•Start Wireshark; Open the trace file ; Apply DNS in the filter window

•Analyse

Write down the following

1. IP address of the client ?

**Ans : 192.168.1.102**

1. IP address of the DNS

**Ans : 63.240.76.19**

**DNS query**

1. Source port in UDP

**Ans : 1026**

1. Destination port in UDP

Ans : 53

1. Is DNS search recursive or iterative ( Check the flags )

**Ans : Recursive**

1. What is the query ?

**Ans : gaia.cs.umass.edu:type A,class IN**

**DNS Reply**

1. How many Authoritative Resource Records?

**Ans :05**

1. How many Additional Resource Records?

**Ans : 05**

1. What is the IP address returned in the reply?

**Ans : 128.119.254.12**

# Protocol : HTTP

Client

Server

Request#1

Reply #1

Request #2

Reply #2

# Protocol : HTTP

Enter HTTP in the filter, Analyse and answer the questions **Request #1 :**

1. What is the browser used in the client?

**Ans : Mozilla/5.0**

1. What is the name of the server ?

**Ans : gaia.cs.umass.edu\r\n**

1. What is the name of the file requested?

**Ans : Get/ethereal-labs/lab2-1.html**

1. Is the connection persistent or non-persistent ?

**Ans : Persistent**

# Reply #1

1. What is the size of the content returned ?

**Ans : Content length :73 Total length : 439**

1. What is the main text content of the reply ?

**Ans : Content length : 73**

**200 OK, Congratulations you have downloaded the file lab2-1.html**

**Request #2**

1. What is the name of the file requested?

Ans : /favicon.ico

# Reply #2

1. What is the reply in the status?

**Ans : 404**

1. What is the size of the contents replied?

**Ans : content length : 1071**

**Total length : 1395**

## Protocol : TCP

## Apply TCP in the filter window

1. Analyse
   1. Connection establishment phase
   2. Data transfer phase
2. Fill up the values for the attributes mentioned in the next slide Primarily Seq & Ack analysis

## Protocol : TCP

Client

IP add :192.168.1.102

:::192.168.1.102

Server

IP add : 128.119.245.12

Seq

No: 0

Seq

No: 0

Syn

flag : 1

Ack

No:1

Syn

Flag: 1

Window size: 64240

Window Size: 5840

Ack

Flag: 1

Seq

No: 1

Ack

No: 1

Seq

No: 1

Ack

No: 502

Seq

No: 989

Ack

No: 1727