Protocol Analysis
Experiment #1
Protocols : HTTP, DNS & TCP

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

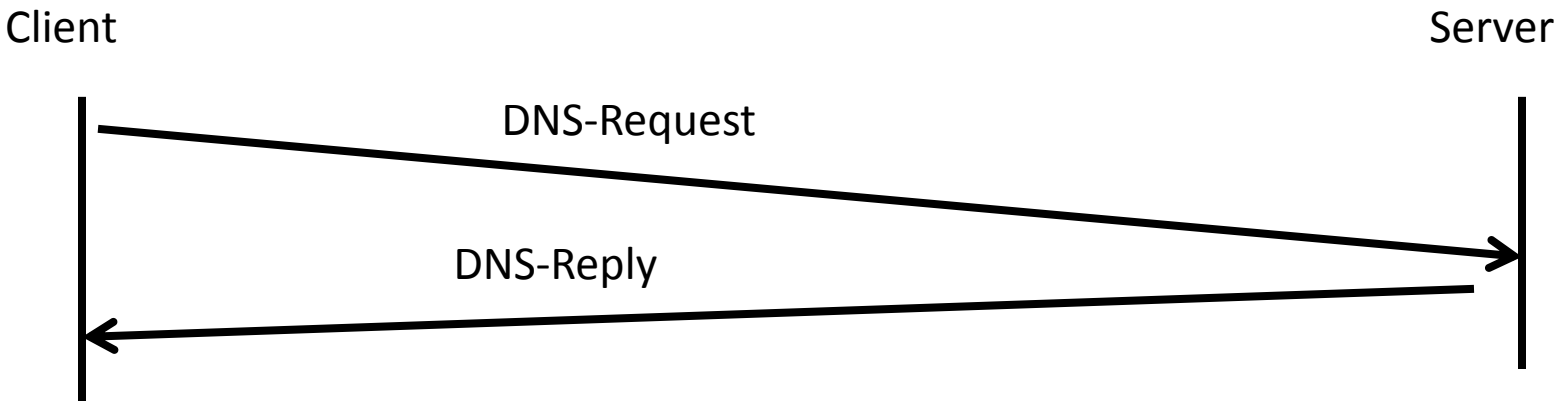
Part#1 : DNS

Part #2 : HTTP

Part #3 : TCP

Trace File to be analysed : HTTP-Tracefiles\http-trace-1

Protocol Analysis Experiment #1
Part#1 : Protocol - DNS



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

•Alnalyse

Write down the following

1. IP address of the client ?
2. IP address of the DNS

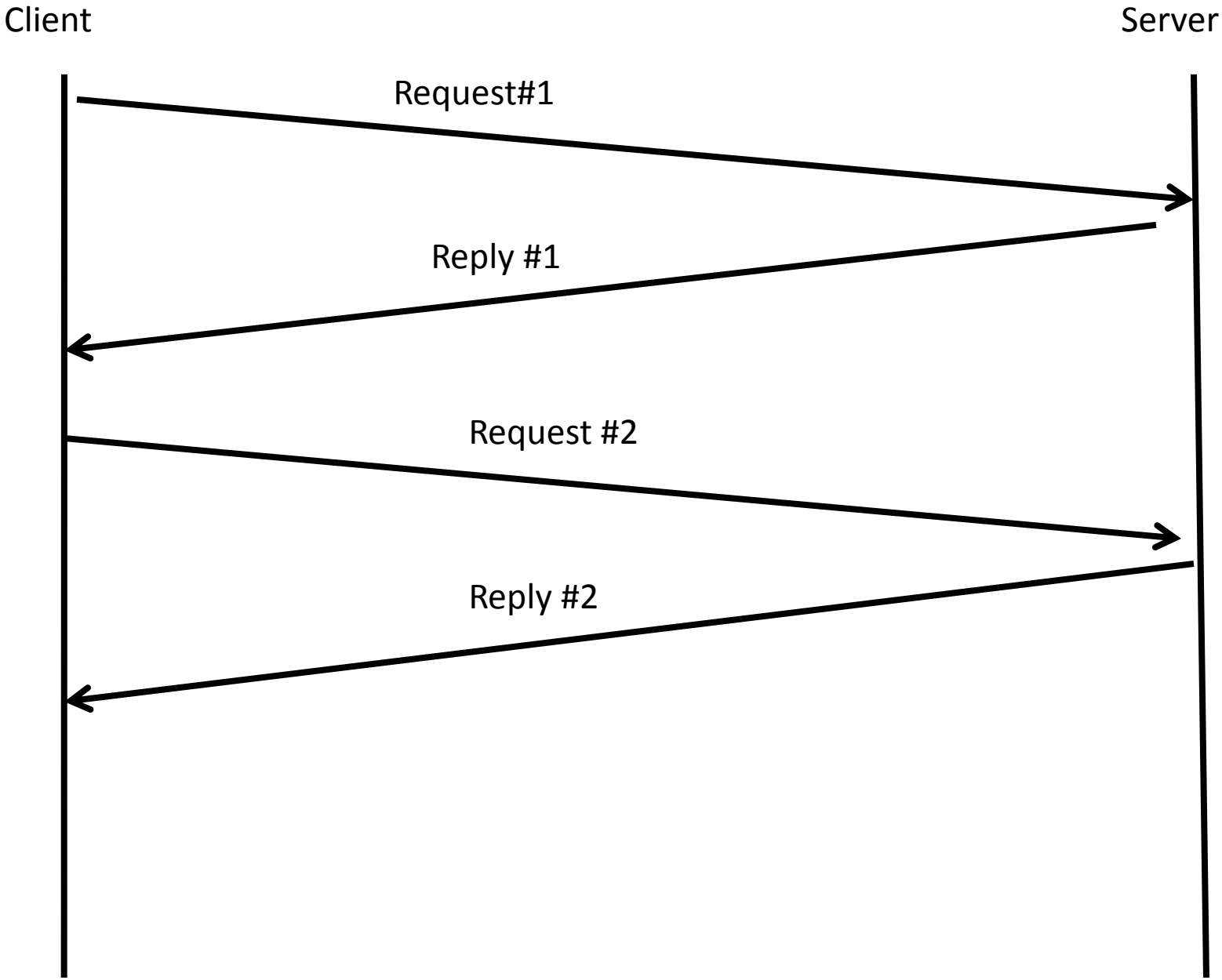
DNS query

1. Source port in UDP
2. Destination port in UDP
3. Is DNS search recursive or iterative (Check the flags)
4. What is the query ?

DNS Reply

1. How many Authoritative Resource Records?
2. How many Additional Resource Records?
3. What is the IP address returned in the reply?

Protocol Analysis Experiment #1
Protocol : HTTP



Protocol Analysis Experiment #1
Protocol : HTTP

Enter HTTP in the filter, Analyse and answer the questions

Request #1 :

1. What is the browser used in the client?
2. What is the name of the server ?
3. What is the name of the file requested?
4. Is the connection persistent or non-persistent ?

Reply #1

1. What is the size of the content returned ?
2. What is the main text content of the reply ?

Request #2

1. What is the name of the file requested?

Reply #2

1. What is the reply in the status?
2. What is the size of the contents replied?

Protocol Analysis Experiment #1
Protocol : TCP

1. Apply TCP in the filter window
2. Analyse
    1. Connection establishment phase
    2. Data transfer phase

3. Fill up the values for the attributes mentioned in the next slide
Primarily Seq & Ack analysis

Protocol Analysis Experiment #1
Protocol : TCP