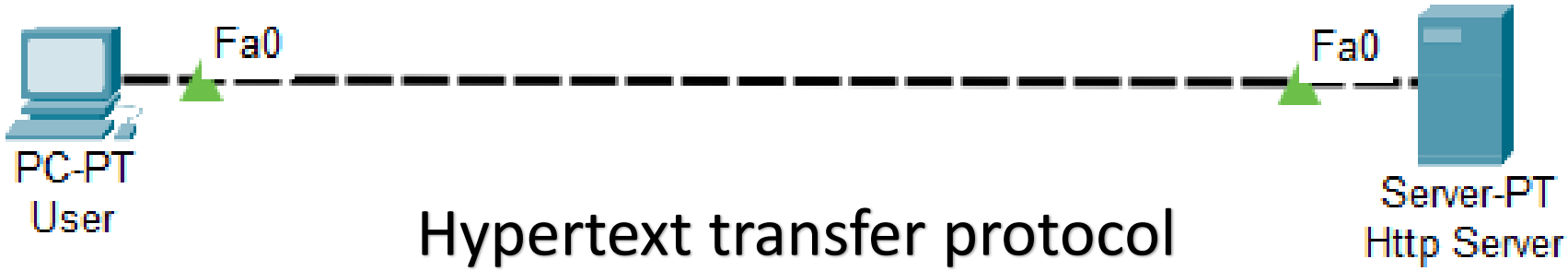
Balayogi Gnanasekar

HTTP Protocol



Hypertext transfer protocol

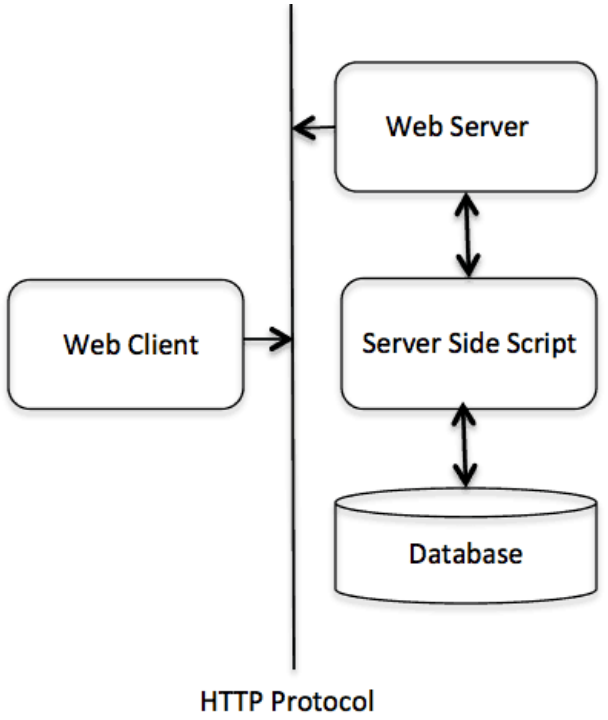
Balayogi G

HTTP Overview

- Application layer protocol.
- TCP/IP based communication protocol, delivers data such as Image, Video, Audio, HTML pages, etc.,
- Distributed, collabrative and hypermedia transmission system.
- Foundation for World wide web(WWW) since 1990.
- Generic and stateless protocol.
- Standard port for HTTP protocol on TCP is 80(Other ports can also be used).
- Connectionless protocol.
- Media independent.
- Stateless protocol.
- Types: HTTP/1 and HTTP/2.

HTTP Overview(cont.)

- HTTP/1.0 uses a new connection for each request/response exchange, where as HTTP/1.1 connection may be used for one or more request/response exchanges.
- Request / Response based protocol.
- For example, web browsers, robots, search engines and more.



HTTP Parameters

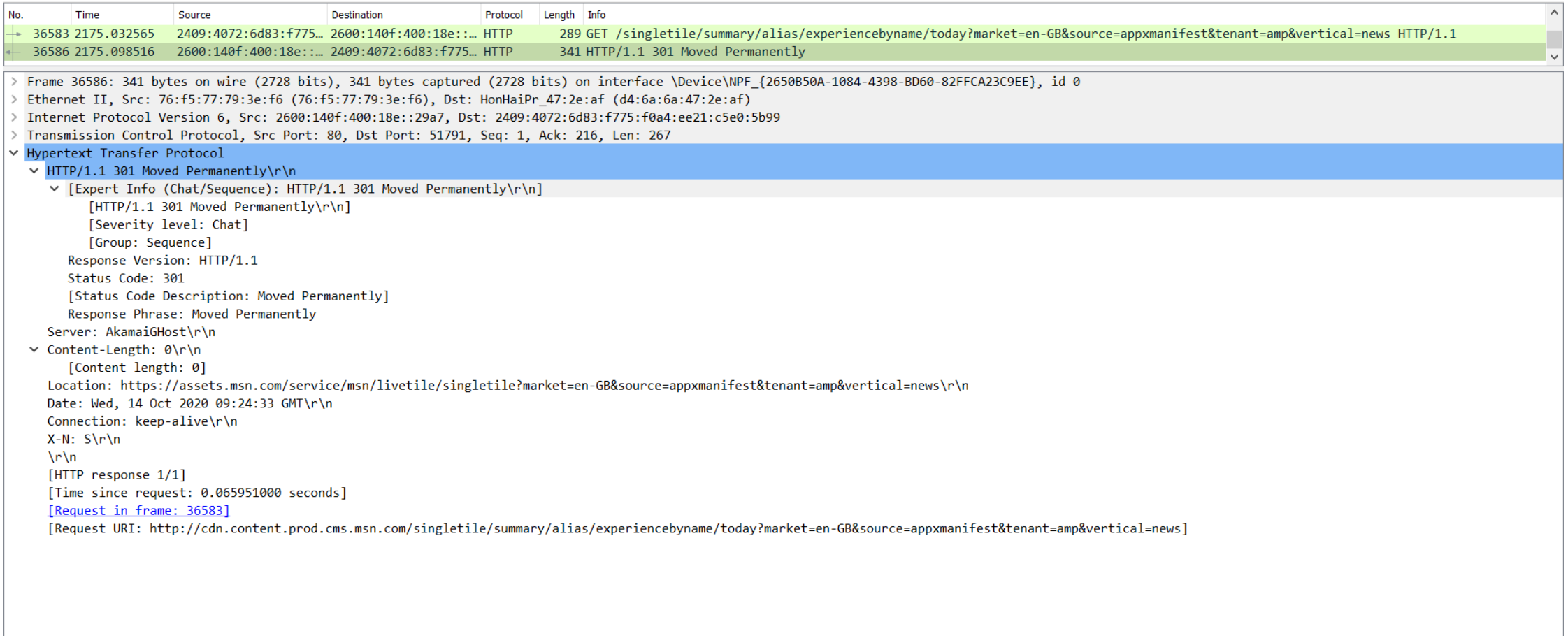
- HTTP version
- URI – Uniform resource locator
- Date / time format
- Character sets
- Content encoding
- Media types
- Language tags

HTTP Request packet capture

No.	Time	Source	Destination	Protocol	Length	Info
249	-8.275140	2409:4072:6d83:f775…	2404:6800:4007:803:…	HTTP	784	GET / HTTP/1.1
258	-8.162457	2404:6800:4007:803:…	2409:4072:6d83:f775…	HTTP	602	HTTP/1.1 301 Moved Permanently (text/html)

```
> Frame 249: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF_{2650B50A-1084-4398-BD60-82FFCA23C9EE}, id 0
> Ethernet II, Src: HonHaiPr_47:2e:af (d4:6a:6a:47:2e:af), Dst: 76:f5:77:79:3e:f6 (76:f5:77:79:3e:f6)
> Internet Protocol Version 6, Src: 2409:4072:6d83:f775:f0a4:ee21:c5e0:5b99, Dst: 2404:6800:4007:803::200e
> Transmission Control Protocol, Src Port: 51226, Dst Port: 80, Seq: 1, Ack: 1, Len: 710
v Hypertext Transfer Protocol
  v GET / HTTP/1.1\r\n
    v [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
        [GET / HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
    Host: google.com\r\n
    Connection: keep-alive\r\n
    DNT: 1\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,en-GB;q=0.8\r\n
  v [truncated]Cookie: SID=2QeLU7U6j3zgjv-HNCJI0M2HmFHBLAsvQl1YHpPihQVoEFH0sYf34QPlc_seJDhf1at1Jg.; HSID=AJNPZu2q0ftx3uUVG; APISID=15eNnZpOvbjynJ9H/A-2HhK3Bhx6bDP6AX; SEARCH_SAMESITE=CgQI9ZAB; SIDCC=AJi4QfHxa…
      Cookie pair: SID=2QeLU7U6j3zgjv-HNCJI0M2HmFHBLAsvQl1YHpPihQVoEFH0sYf34QPlc_seJDhf1at1Jg.
      Cookie pair: HSID=AJNPZu2q0ftx3uUVG
      Cookie pair: APISID=15eNnZpOvbjynJ9H/A-2HhK3Bhx6bDP6AX
      Cookie pair: SEARCH_SAMESITE=CgQI9ZAB
      Cookie pair: SIDCC=AJi4QfHxacIlPkN037hAEUgTyPKSTXQNGCpJz6QqRYzhwbJcHqMld9jkZWm5qMR_9bY0-_wDyW0
    \r\n
    [Full request URI: http://google.com/]
    [HTTP request 1/1]
    [Response in frame: 258]
```

HTTP Response Packet capture



No.	Time	Source	Destination	Protocol	Length	Info
36583	2175.032565	2409:4072:6d83:f775…	2600:140f:400:18e::…	HTTP	289	GET /singletile/summary/alias/experiencebyname/today?market=en-GB&source=appxmanifest&tenant=amp&vertical=news HTTP/1.1
36586	2175.098516	2600:140f:400:18e::…	2409:4072:6d83:f775…	HTTP	341	HTTP/1.1 301 Moved Permanently

```
> Frame 36586: 341 bytes on wire (2728 bits), 341 bytes captured (2728 bits) on interface \Device\NPF_{2650B50A-1084-4398-BD60-82FFCA23C9EE}, id 0
> Ethernet II, Src: 76:f5:77:79:3e:f6 (76:f5:77:79:3e:f6), Dst: HonHaiPr_47:2e:af (d4:6a:6a:47:2e:af)
> Internet Protocol Version 6, Src: 2600:140f:400:18e::29a7, Dst: 2409:4072:6d83:f775:f0a4:ee21:c5e0:5b99
> Transmission Control Protocol, Src Port: 80, Dst Port: 51791, Seq: 1, Ack: 216, Len: 267
v Hypertext Transfer Protocol
  v HTTP/1.1 301 Moved Permanently\r\n
    v [Expert Info (Chat/Sequence): HTTP/1.1 301 Moved Permanently\r\n]
        [HTTP/1.1 301 Moved Permanently\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Response Version: HTTP/1.1
      Status Code: 301
      [Status Code Description: Moved Permanently]
      Response Phrase: Moved Permanently
    Server: AkamaiGHost\r\n
  v Content-Length: 0\r\n
      [Content length: 0]
    Location: https://assets.msn.com/service/msn/livetile/singletile?market=en-GB&source=appxmanifest&tenant=amp&vertical=news\r\n
    Date: Wed, 14 Oct 2020 09:24:33 GMT\r\n
    Connection: keep-alive\r\n
    X-N: S\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.065951000 seconds]
    [Request in frame: 36583]
    [Request URI: http://cdn.content.prod.cms.msn.com/singletile/summary/alias/experiencebyname/today?market=en-GB&source=appxmanifest&tenant=amp&vertical=news]
```

HTTP Messages

- HTTP requests and HTTP responses use a generic message format of RFC 822 for transferring the required data. This generic message format consists of the following four items.
  - A Start-line
  - Zero or more header fields followed by CRLF(**\r or carriage return**)
  - An empty line (i.e., a line with nothing preceding the CRLF) indicating the end of the header fields
  - Optionally a message-body

HTTP Methods

Method	Description
GET	To retrive information from server.
HEAD	Similar to GET, but retrives only status line and header sections.
POST	To send information to server.
PUT	Replacing all the current representation of target resource in the server.
DELETE	Removes all current representations of the target resource given by a URI.
CONNECT	Establish the tunnel to the server given by URI.
OPTIONS	Describes the communication options for the target resource.
TRACE	Performs a message loop-back test along the path to the target resource.

HTTP Status codes

Status code	Description
1XX	**Informational Error** It means the request has been received and the process is continuing.
2XX	**Success** It means the action was successfully received, understood, and accepted.
3XX	**Redirection** It means further action must be taken in order to complete the request.
4XX	**Client Error** It means the request contains incorrect syntax or cannot be fulfilled.
5XX	**Server Error** It means the server failed to fulfill an apparently valid request.

HTTP – Information Error

Error Message	Description
100 Continue	When only a part of the request has been received by the server, but until the request is not been rejected, client can continue sending other parts of request.
101 Switching protocols	When the server switch protocols.

HTTP – Success

Error Message	Description
200 OK	Request is OK
201 Created	Request is complete and a new resource is created
202 Accepted	Request is accepted for processing, but the processing is not complete.
203 Non-authoritative information	Information in the entity header is from local or third party copy and not from the original server.
204 No content	Status code and a header are given in the response, but there is not entity body in the reply.
205 Reset content	Browser should clear the form used for this transaction for additional input.
206 Partial content	Server returned a partial data of the size of requested. The requested range is given in **Range header**, and the **content-Range header** will be in response.

HTTP – Redirection

Error Message	Description
300 Multiple choices	A link list. The user can select a link and go to that location. Maximum five addresses.
301 Moved permanently	The requested page has moved to a new url .
302 Found	The requested page has moved temporarily to a new url .
303 See other	The requested page can be found under a different url .
304 Not modified	This is the response code to an *If-Modified-Since* or *If-None-Match* header, where the URL has not been modified since the specified date.
305 use proxy	The requested URL must be accessed through the proxy mentioned in the *Location* header.
306 unused	This code was used in a previous version. It is no longer used, but the code is reserved.
307 Temporiary redirect	The requested page has moved temporarily to a new url .

HTTP – Client Error

Error Message	Description
400 Bad Request	The server did not understand the request.
401 Unauthorized	The requested page needs a username and a password.
402 Payment required	You can not use this code yet.
403 Forbidden	Access is forbidden to the requested page.
404 Not found	The server can not find the requested page.
405 Method not found	The method specified in the request is not allowed.
406 Not acceptable	The server can only generate a response that is not accepted by the client.
407 Proxy authentication required	You must authenticate with a proxy server before this request can be served.
408 Request Time out	The request took longer than the server was prepared to wait.

HTTP – Client Error(Cont.)

Error Message	Description
409 Conflict	The request could not be completed because of a conflict.
410 Gone	The requested page is no longer available .
411 Length Required	The "Content-Length" is not defined. The server will not accept the request without it .
412 Precondition failed	The pre condition given in the request evaluated to false by the server.
413 Request Entity too large	The server will not accept the request, because the request entity is too large.
414 Request URL too long	The server will not accept the request, because the url is too long. Occurs when you convert a "post" request to a "get" request with a long query information .

HTTP – Client Error(Cont.)

Error Message	Description
415 Unsupported Media type	The server will not accept the request, because the mediatype is not supported .
416 Requested range not satisfiable	The requested byte range is not available and is out of bounds.
417 Expectation failed	The expectation given in an Expect request-header field could not be met by this server.

HTTP – Server Error

Error Message	Description
500 Internal server error	The request was not completed. The server met an unexpected condition.
501 Not implemented	The request was not completed. The server did not support the functionality required.
502 Bad gateway	The request was not completed. The server received an invalid response from the upstream server
503 Service Unavaiable	The request was not completed. The server is temporarily overloading or down.
504 Gateway time out	The gateway has timed out.
505 HTTP version not supported	The server does not support the "http protocol" version.

HTTP – Headers

HTTP header fields provide required information about the request or response, or about the object sent in the message body. There are four types of HTTP message headers:

- **General-header:** These header fields have general applicability for both request and response messages.
- **Client Request-header:** These header fields have applicability only for request messages.
- **Server Response-header:** These header fields have applicability only for response messages.
- **Entity-header:** These header fields define meta information about the entity-body or, if no body is present, about the resource identified by the request.

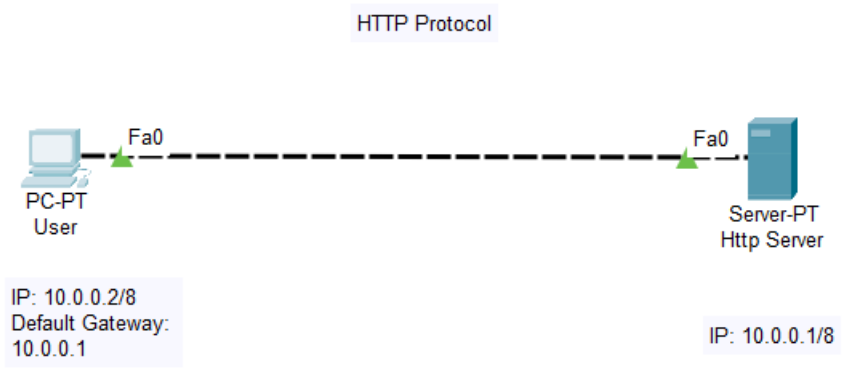
HTTP Security

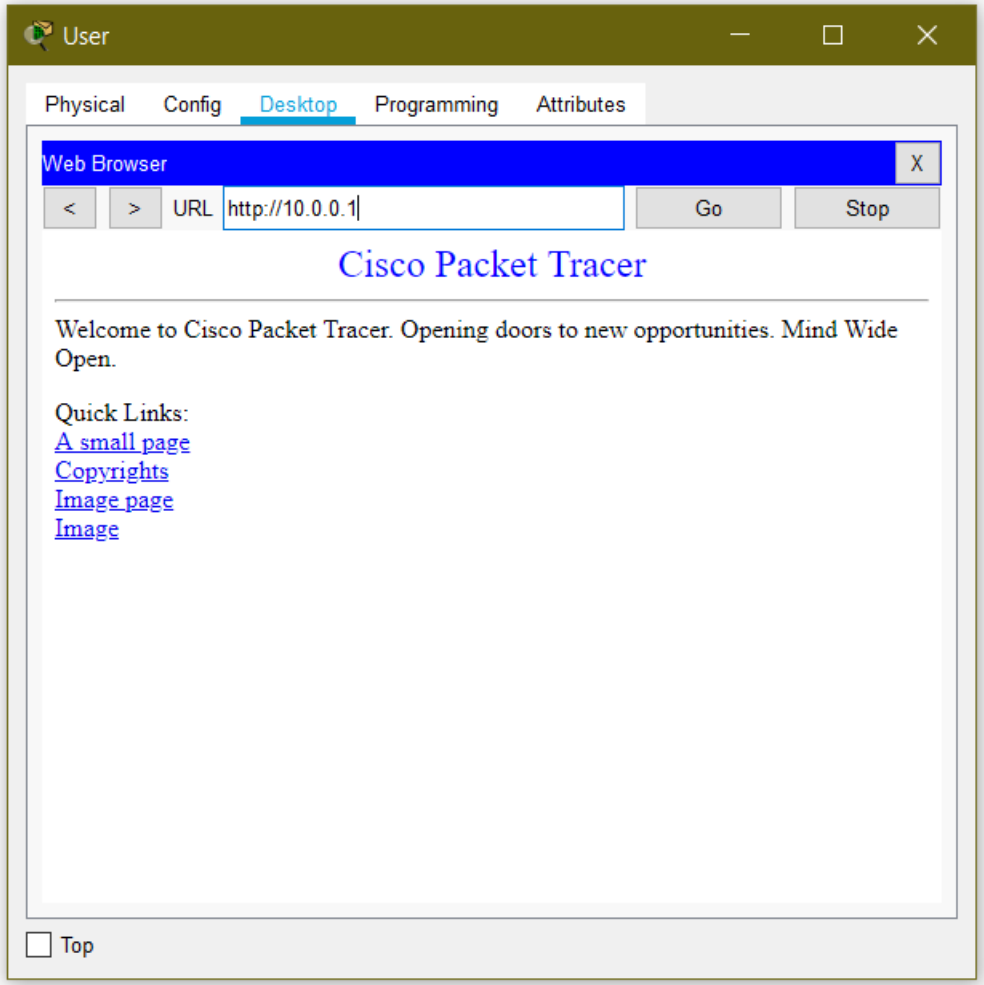
- **Personal information leakage**
  - HTTP clients are often privy to large amount of personal information such as the user's name, location, mail address, passwords, encryption keys, etc. So you should be very careful to prevent unintentional leakage of this information via the HTTP protocol to other sources.
- **File and Path name based attack or Directory traversal**
  - Directory traversal (also known as file path traversal) is a web security vulnerability that allows an attacker to read arbitrary files on the server that is running an application. This might include application code and data, credentials for back-end systems, and sensitive operating system files.
- **DNS Spoofing**
  - DNS spoofing occurs when a particular DNS server's records of "spoofed" or altered maliciously to redirect traffic to the attacker. This redirection of traffic allows the attacker to spread malware, steal data, etc
- **Location Header and Spoofing**
  - Header spoofing is when a URL appears to be downloaded from a certain domain, but in reality it is downloaded from a different and (very likely) malicious one. Unlike other types of spoofing techniques, this action is done without any system or file modification.

HTTP Security(Cont.)

- **Authentication credientals**
  - Existing HTTP clients and user agents typically retain authentication information indefinitely. HTTP/1.1 does not provide a method for a server to direct clients to discard these cached credentials which is a big security risk.
- **Proxies and cacheing**
  - HTTP proxies are men-in-the-middle, and represent an opportunity for man-in-the-middle attacks. Proxies have access to security-related information, personal information about individual users and organizations, and proprietary information belonging to users and content providers.
  - Proxy operators should protect the systems on which proxies run, as they would protect any system that contains or transports sensitive information.
  - Caching proxies provide additional potential vulnerabilities, since the contents of the cache represent an attractive target for malicious exploitation. Therefore, cache contents should be protected as sensitive information.

HTTP Implementation





Thanks for watching...☺