sait.ca

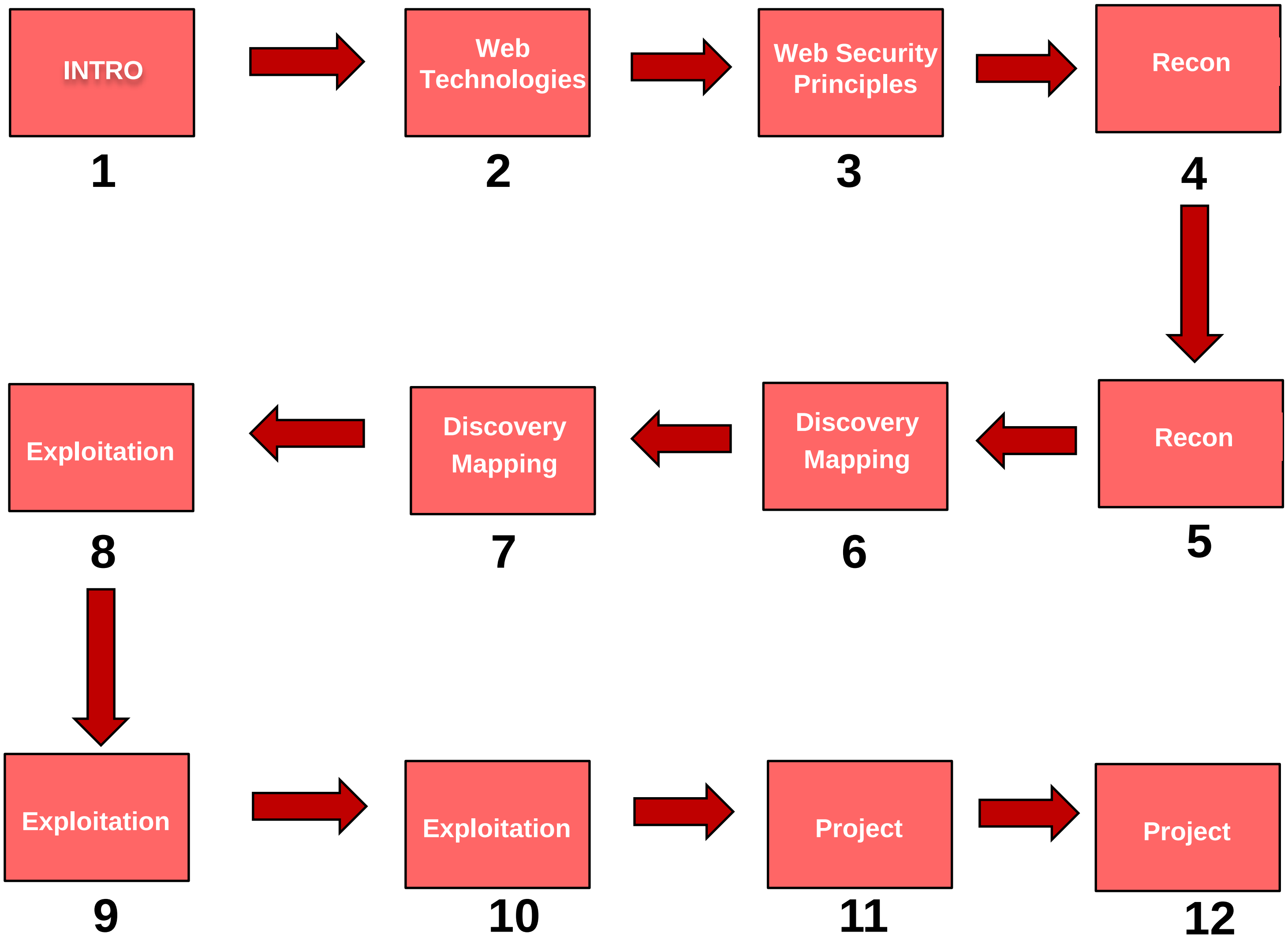
SAIT POLYTECHNIC

FURTHER YOUR PASSION

Web App & Data Base Security

Web Tech

Web App & Data Base Security



INTRO
1

Web Technologies
2

Web Security Principles
3

Recon
4

Recon
5

Discovery Mapping
6

Discovery Mapping
7

Exploitation
8

Exploitation
9

Exploitation
10

Project
11

Project
12

Agenda

- Web Servers;
- The HTTP Protocol;
- HTTP Request;
- HTTP Response;
- User-agents;
- Lab 1 – Understanding HTTP Protocol using Wireshark;
- Lab 2 – Analyzing the web servers (reviewing some tools).

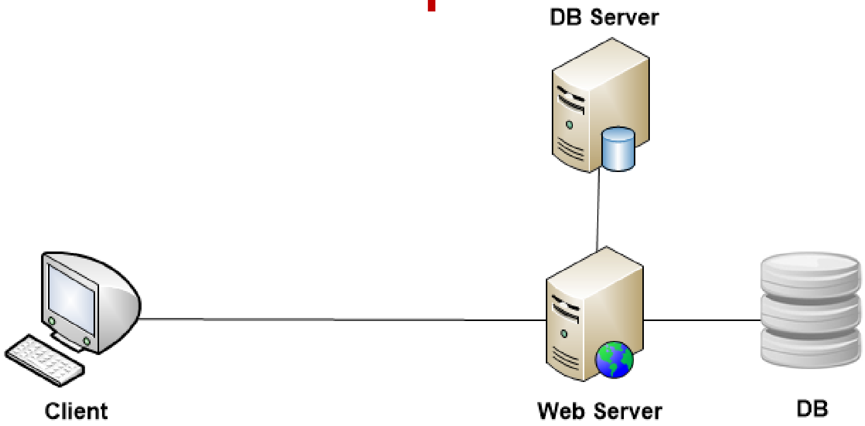
Web Servers

- Pure Web Servers are rare today;
- They server static content only;
- Typically safe from most active web application attacks;
- Most modern web servers fall under the hybrid category.

Client
Web Server

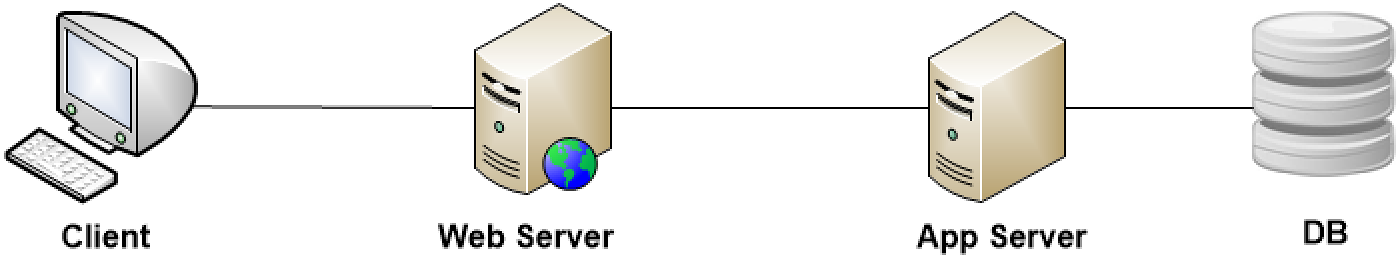
Dynamic Server Architecture

- Web Server that serves both static and active content (most common today);
- Active content often drawn from a back-end data base (Commonly a relational data base using SQL);
- Mode difficult to protect and harden.



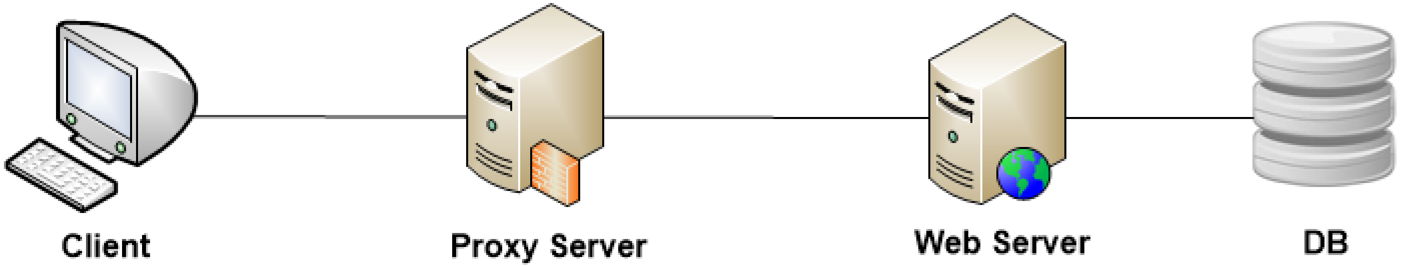
Application Servers

- Applications run within a server application (WebSphere, BEA WebLogic, Jboss, Tomcat);
- App Servers usually don't communicate directly with the clients.



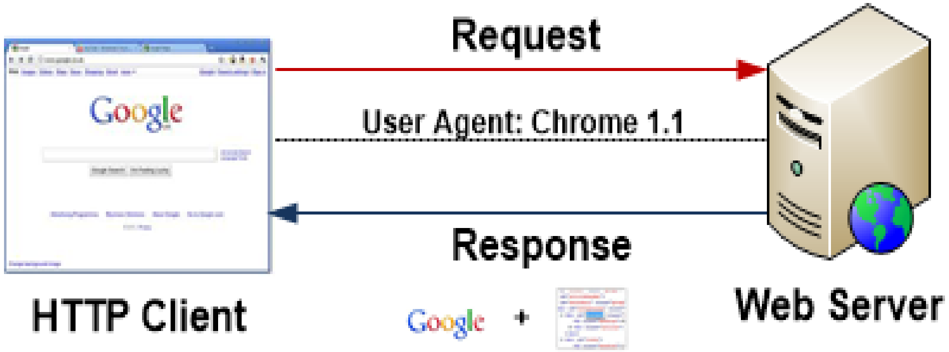
Proxy Servers Architecture

- A proxy server front ends for one or more application (called reverse proxy);
- The proxy passed requests thru the application and caches the results;
- Adds one more layer of protection.



The HTTP Protocol

- Hypertext Transport Protocol;
- Language of the Web:
  - protocol used for communication between web browsers and web servers;
- Request-Response pattern;
- Client-Server model;
- TCP port 80.



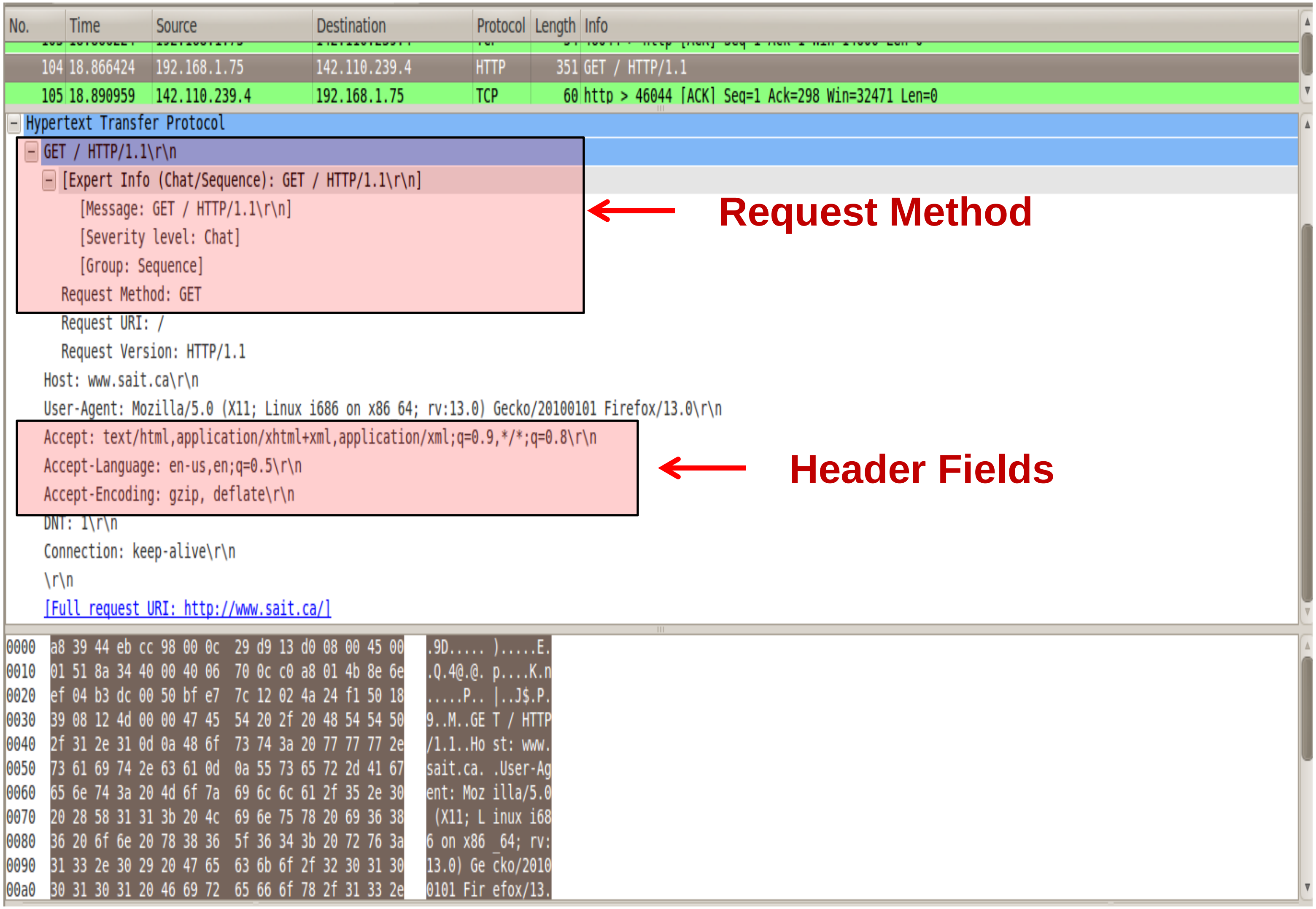
HTTP Request Packets

- Sent from client to server;
- Consists of HTTP header:
  - – header is hidden in browser environment
  - – contains:
    - content type;
    - content length;
    - user agent - browser issuing request;
    - content types user agent can handle.
- and a URL.

HTTP Request Headers

- Precede HTTP Method requests;
- Headers are terminated by a blank line;
- Header Fields:
  - From;
  - Accept;
  - Accept-Encoding;
  - Accept Language.

HTTP Request Headers



```
No.   Time       Source          Destination     Protocol Length Info
  104 18.866424  192.168.1.75    142.110.239.4   HTTP        351 GET / HTTP/1.1
  105 18.890959  142.110.239.4   192.168.1.75    TCP          60 http > 46044 [ACK] Seq=1 Ack=298 Win=32471 Len=0
```

```
− Hypertext Transfer Protocol
  − GET / HTTP/1.1\r\n
    − [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
        [Message: GET / HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /
      Request Version: HTTP/1.1
    Host: www.sait.ca\r\n
    User-Agent: Mozilla/5.0 (X11; Linux i686 on x86 64; rv:13.0) Gecko/20100101 Firefox/13.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    DNT: 1\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://www.sait.ca/]
```

```
0000  a8 39 44 eb cc 98 00 0c  29 d9 13 d0 08 00 45 00   .9D..... ).....E.
0010  01 51 8a 34 40 00 40 06  70 0c c0 a8 01 4b 8e 6e   .Q.4@.@. p....K.n
0020  ef 04 b3 dc 00 50 bf e7  7c 12 02 4a 24 f1 50 18   .....P.. |..J$.P.
0030  39 08 12 4d 00 00 47 45  54 20 2f 20 48 54 54 50   9..M..GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 77 77 77 2e   /1.1..Ho st: www.
0050  73 61 69 74 2e 63 61 0d  0a 55 73 65 72 2d 41 67   sait.ca. .User-Ag
0060  65 6e 74 3a 20 4d 6f 7a  69 6c 6c 61 2f 35 2e 30   ent: Moz illa/5.0
0070  20 28 58 31 31 3b 20 4c  69 6e 75 78 20 69 36 38    (X11; L inux i68
0080  36 20 6f 6e 20 78 38 36  5f 36 34 3b 20 72 76 3a   6 on x86 _64; rv:
0090  31 33 2e 30 29 20 47 65  63 6b 6f 2f 32 30 31 30   13.0) Ge cko/2010
00a0  30 31 30 31 20 46 69 72  65 66 6f 78 2f 31 33 2e   0101 Fir efox/13.
```

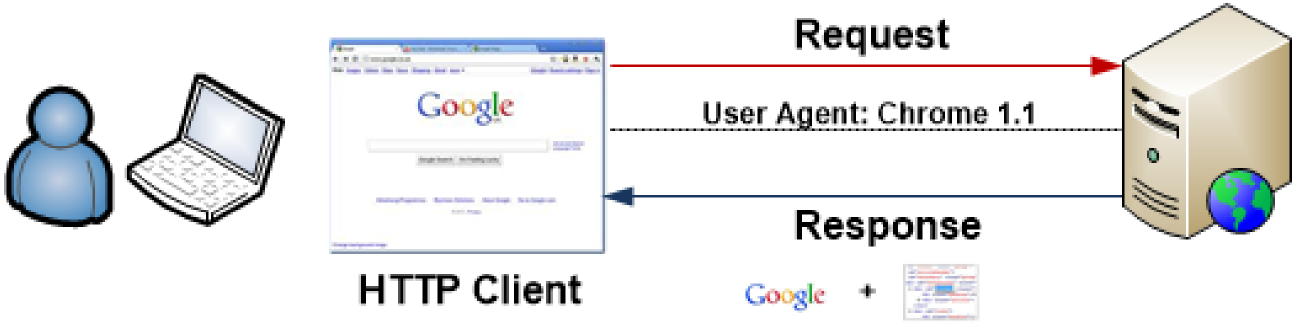
Request Method

Header Fields

HTTP Request Methods

GET – retrieve document specified by URL;

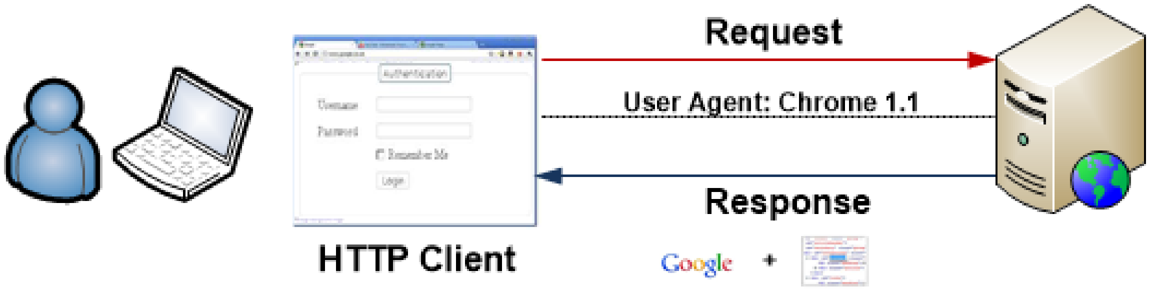
```
GET /index.html?report_id=34543222 HTTP/1.1
Host: www.sait230.ca
User-Agent: Chrome/1.1
```



HTTP Request Methods

POST – give information (eg. annotation) to the server. Preferred method for forms processing;

```
POST /login.jsp HTTP/1.1
Host: www.sait230.ca
User-Agent: Chrome/1.1
Content-Length: 27
Content-Type: application/x-www-form-urlencoded
userid=mo&password=mypassw
```



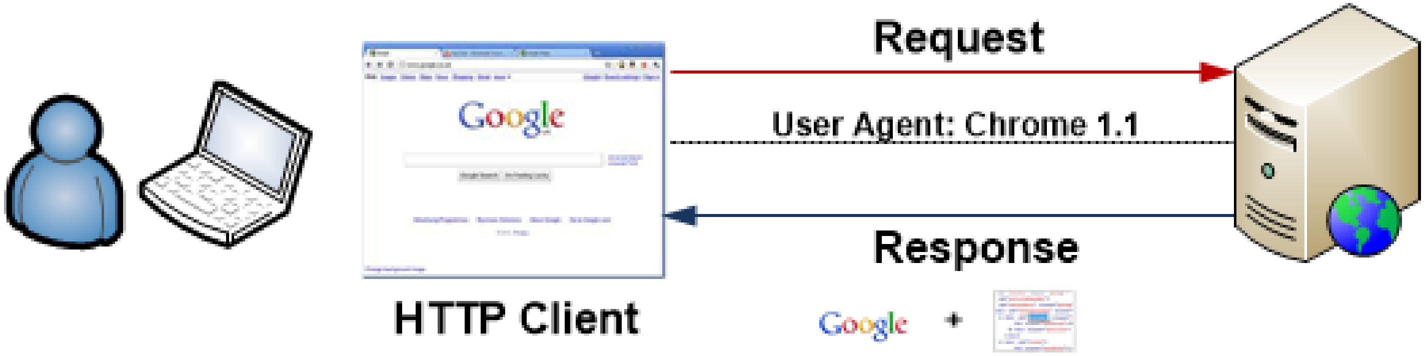
HTTP Request Methods

- PUT:
- HEAD:
- OPTIONS:
- DELETE:
- TRACE:
- CONNECT:

Home Work!

HTTP Response

- The server responds to the client with the status code and message;
- It will return a content type to tell the client what type of data to expect and a content length.



HTTP Response Headers

- Sent by server to client browser;
- Status Header;
  - Entities
    - Content-Encoding;
    - Content-Length: length of the response;
    - Content-Type;
    - Expires;
    - Last-Modified;
    - extension-header.
- Body – content (usually html)

HTTP Status Codes

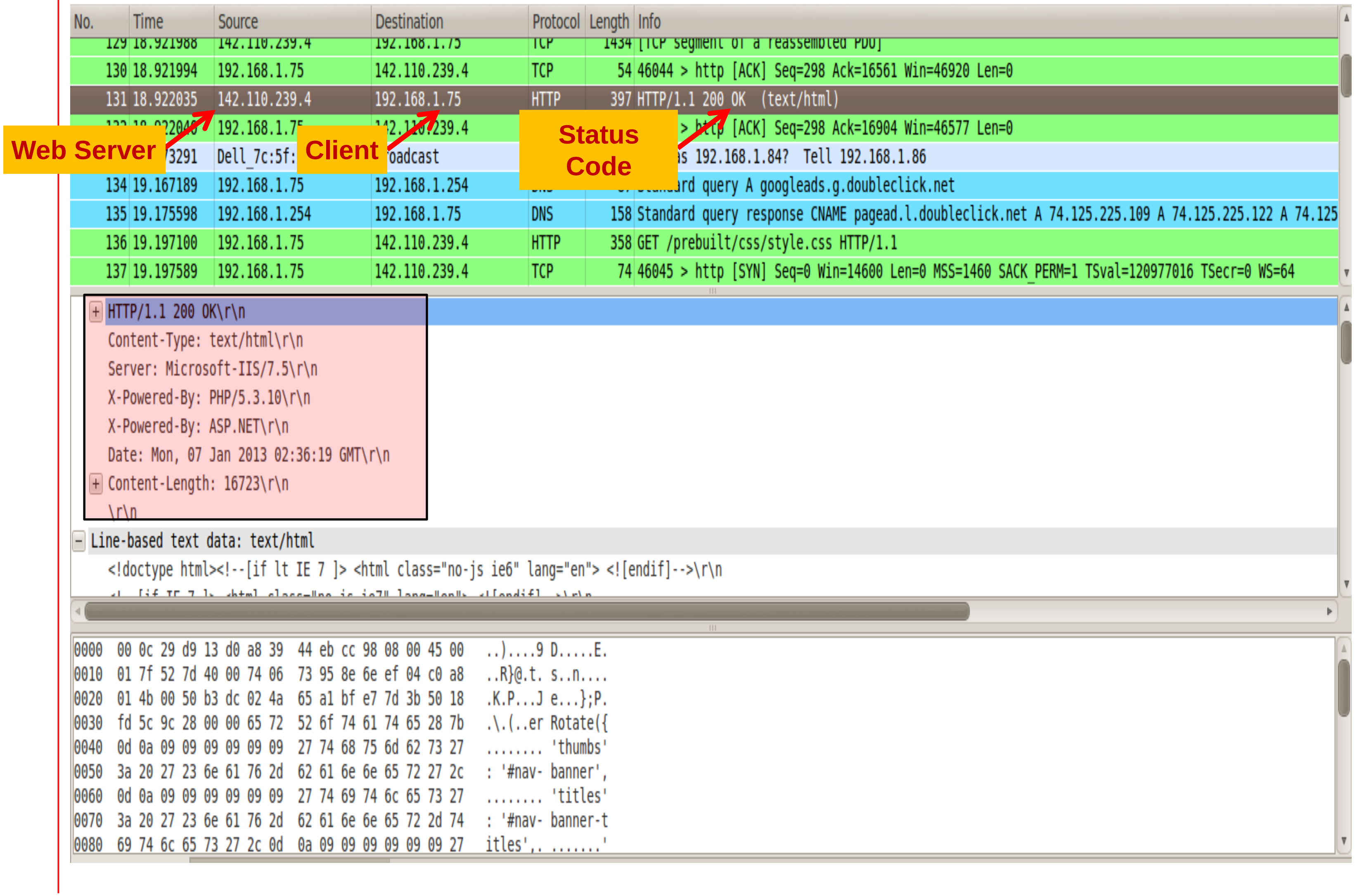
It is a code that tells the status of the request:

- 1xx – Informational – request received;
- 2xx – Success – action received;
- 3xx – Redirection – further action necessary;
- 4xx – Client Error – bad syntax or cannot be fulfilled;
- 5xx – Server Error – server failed.

HTTP Status Codes

- 200 OK
- 201 created
- 202 accepted
- 204 no content
- 301 moved perm.
- 302 moved temp
- 304 not modified
- 400 bad request
- 401 unauthorized
- 403 forbidden
- 404 not found
- 500 int. server error
- 501 not impl.
- 502 bad gateway
- 503 svc not avail

HTTP Response Headers



Web Server

Client

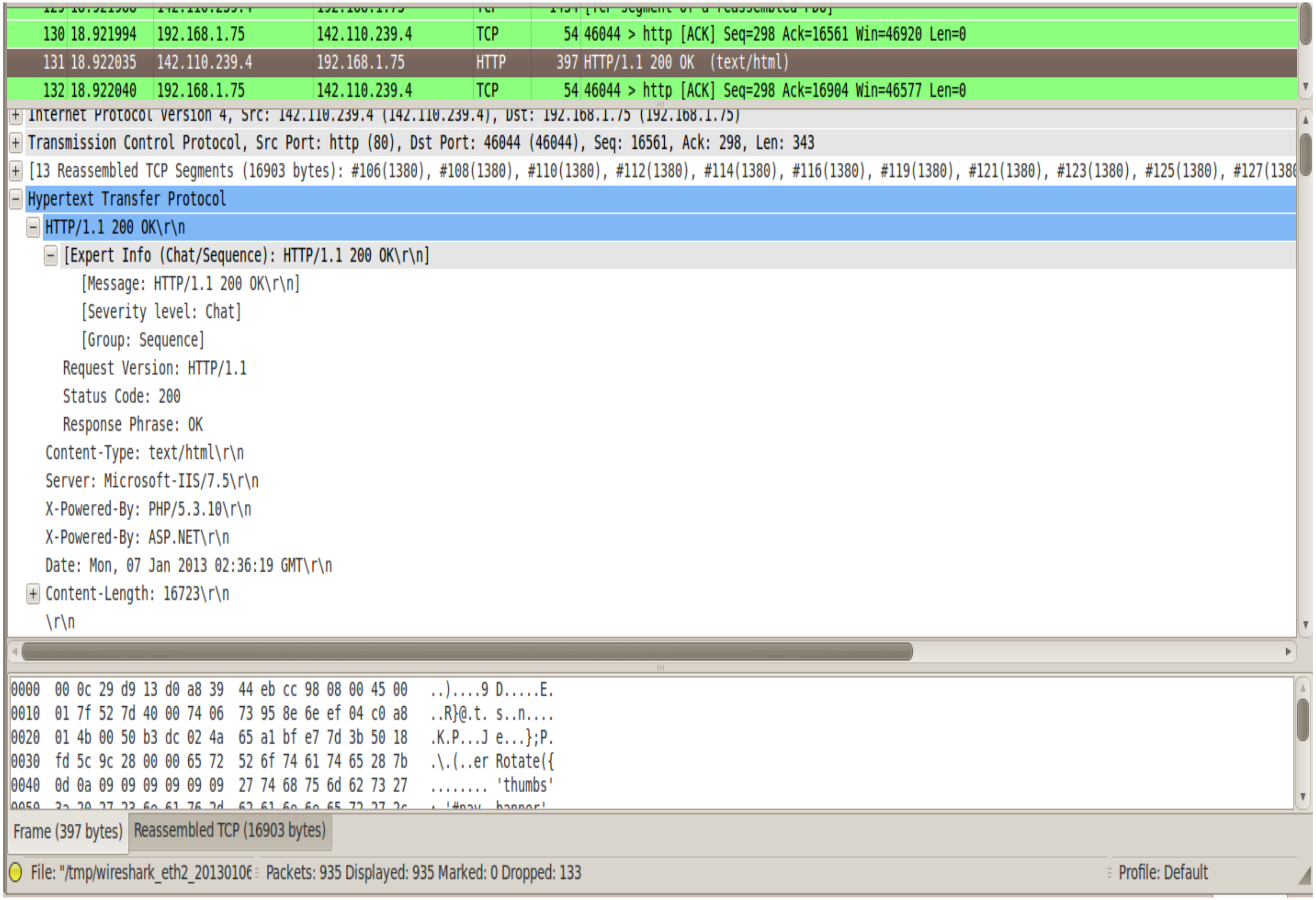
Status Code

```
No.  Time       Source          Destination     Protocol Length Info
 129 18.921988  142.110.239.4   192.168.1.75    TCP      1434 [TCP segment of a reassembled PDU]
 130 18.921994  192.168.1.75    142.110.239.4   TCP        54 46044 > http [ACK] Seq=298 Ack=16561 Win=46920 Len=0
 131 18.922035  142.110.239.4   192.168.1.75    HTTP      397 HTTP/1.1 200 OK  (text/html)
 1   1  922046  192.168.1.75    142.110.239.4                 > http [ACK] Seq=298 Ack=16904 Win=46577 Len=0
    3291        Dell_7c:5f:     oadcast                       s 192.168.1.84?  Tell 192.168.1.86
 134 19.167189  192.168.1.75    192.168.1.254                  rd query A googleads.g.doubleclick.net
 135 19.175598  192.168.1.254   192.168.1.75    DNS       158 Standard query response CNAME pagead.l.doubleclick.net A 74.125.225.109 A 74.125.225.122 A 74.125
 136 19.197100  192.168.1.75    142.110.239.4   HTTP      358 GET /prebuilt/css/style.css HTTP/1.1
 137 19.197589  192.168.1.75    142.110.239.4   TCP        74 46045 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=120977016 TSecr=0 WS=64
```

```
 + HTTP/1.1 200 OK\r\n
   Content-Type: text/html\r\n
   Server: Microsoft-IIS/7.5\r\n
   X-Powered-By: PHP/5.3.10\r\n
   X-Powered-By: ASP.NET\r\n
   Date: Mon, 07 Jan 2013 02:36:19 GMT\r\n
 + Content-Length: 16723\r\n
   \r\n
- Line-based text data: text/html
   <!doctype html><!--[if lt IE 7 ]> <html class="no-js ie6" lang="en"> <![endif]-->\r\n
   <!--[if IE 7 ]> <html class="no-js ie7" lang="en"> <![endif]-->\r\n
```

```
0000  00 0c 29 d9 13 d0 a8 39  44 eb cc 98 08 00 45 00   ..)....9 D.....E.
0010  01 7f 52 7d 40 00 74 06  73 95 8e 6e ef 04 c0 a8   ..R}@.t. s..n....
0020  01 4b 00 50 b3 dc 02 4a  65 a1 bf e7 7d 3b 50 18   .K.P...J e...};P.
0030  fd 5c 9c 28 00 00 65 72  52 6f 74 61 74 65 28 7b   .\.(..er Rotate({
0040  0d 0a 09 09 09 09 09 09  27 74 68 75 6d 62 73 27   ........ 'thumbs'
0050  3a 20 27 23 6e 61 76 2d  62 61 6e 6e 65 72 27 2c   : '#nav- banner',
0060  0d 0a 09 09 09 09 09 09  27 74 69 74 6c 65 73 27   ........ 'titles'
0070  3a 20 27 23 6e 61 76 2d  62 61 6e 6e 65 72 2d 74   : '#nav- banner-t
0080  69 74 6c 65 73 27 2c 0d  0a 09 09 09 09 09 09 27   itles',. .......'
```

HTTP Response Headers



```
130 18.921994  192.168.1.75   142.110.239.4  TCP    54 46044 > http [ACK] Seq=298 Ack=16561 Win=46920 Len=0
131 18.922035  142.110.239.4  192.168.1.75   HTTP  397 HTTP/1.1 200 OK  (text/html)
132 18.922040  192.168.1.75   142.110.239.4  TCP    54 46044 > http [ACK] Seq=298 Ack=16904 Win=46577 Len=0
```

```
+ Internet Protocol Version 4, Src: 142.110.239.4 (142.110.239.4), Dst: 192.168.1.75 (192.168.1.75)
+ Transmission Control Protocol, Src Port: http (80), Dst Port: 46044 (46044), Seq: 16561, Ack: 298, Len: 343
+ [13 Reassembled TCP Segments (16903 bytes): #106(1380), #108(1380), #110(1380), #112(1380), #114(1380), #116(1380), #119(1380), #121(1380), #123(1380), #125(1380), #127(138
- Hypertext Transfer Protocol
  - HTTP/1.1 200 OK\r\n
    - [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        [Message: HTTP/1.1 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Version: HTTP/1.1
      Status Code: 200
      Response Phrase: OK
    Content-Type: text/html\r\n
    Server: Microsoft-IIS/7.5\r\n
    X-Powered-By: PHP/5.3.10\r\n
    X-Powered-By: ASP.NET\r\n
    Date: Mon, 07 Jan 2013 02:36:19 GMT\r\n
  + Content-Length: 16723\r\n
    \r\n
```

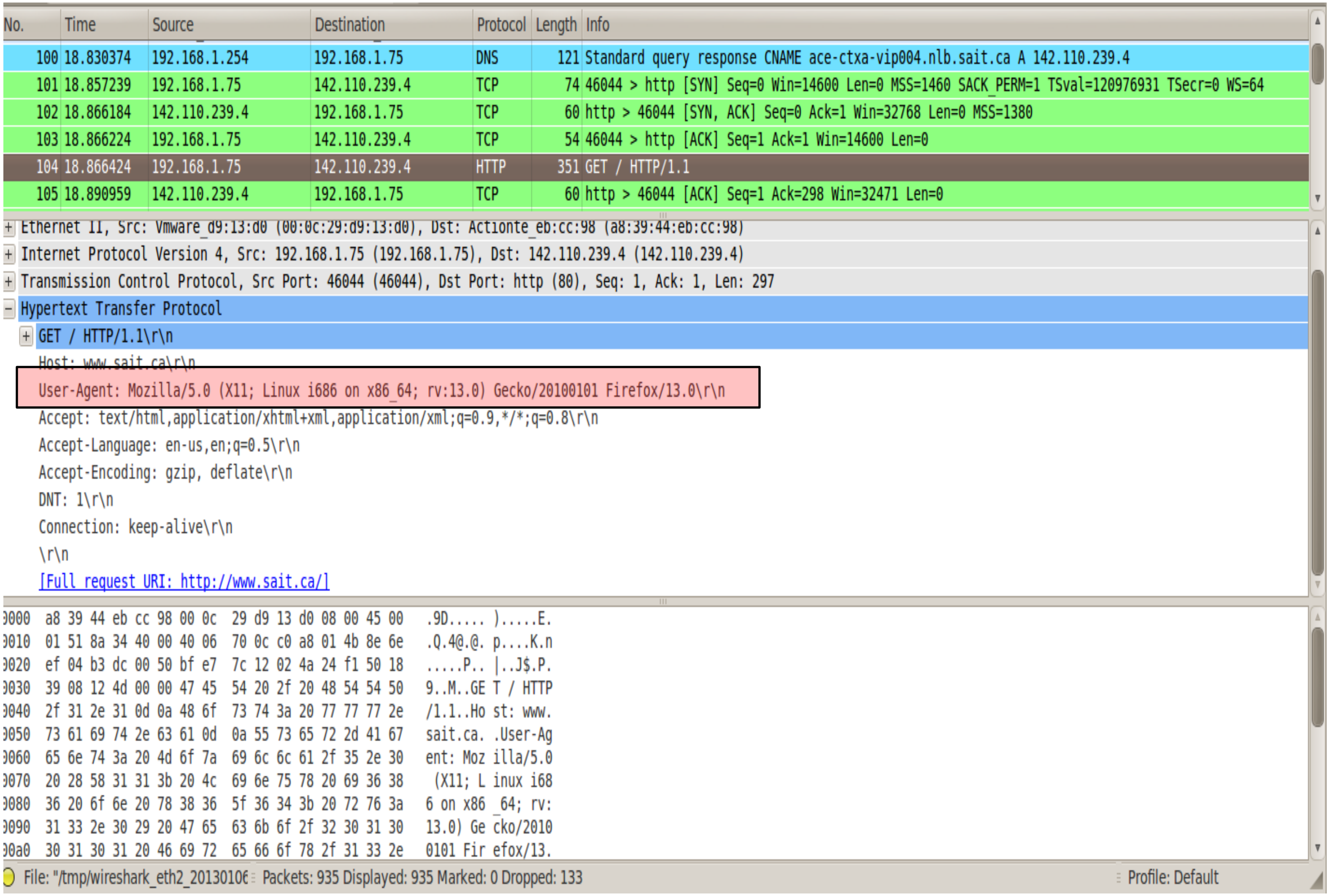
```
0000  00 0c 29 d9 13 d0 a8 39  44 eb cc 98 08 00 45 00   ..)....9 D.....E.
0010  01 7f 52 7d 40 00 74 06  73 95 8e 6e ef 04 c0 a8   ..R}@.t. s..n....
0020  01 4b 00 50 b3 dc 02 4a  65 a1 bf e7 7d 3b 50 18   .K.P...J e...};P.
0030  fd 5c 9c 28 00 00 65 72  52 6f 74 61 74 65 28 7b   .\.(..er Rotate({
0040  0d 0a 09 09 09 09 09 09  27 74 68 75 6d 62 73 27   ........ 'thumbs'
0050  3a 20 27 23 6e 61 76 2d  62 61 6e 6e 65 72 27 2c   : '#nav- banner',
```

Frame (397 bytes)
Reassembled TCP (16903 bytes)
File: "/tmp/wireshark_eth2_2013010€ Packets: 935 Displayed: 935 Marked: 0 Dropped: 133
Profile: Default

User-Agent

- Software product used by original client;
- The HTTP client;
- <field> = User-Agent: <product>
- <product> = <word> [/<version>]
- <version> = <word>
- Ex.
  - User-Agent: Mozilla/5

User-Agent



```
No.  Time       Source         Destination    Protocol Length Info
 100 18.830374  192.168.1.254  192.168.1.75   DNS         121 Standard query response CNAME ace-ctxa-vip004.nlb.sait.ca A 142.110.239.4
 101 18.857239  192.168.1.75   142.110.239.4  TCP          74 46044 > http [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=120976931 TSecr=0 WS=64
 102 18.866184  142.110.239.4  192.168.1.75   TCP          60 http > 46044 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1380
 103 18.866224  192.168.1.75   142.110.239.4  TCP          54 46044 > http [ACK] Seq=1 Ack=1 Win=14600 Len=0
 104 18.866424  192.168.1.75   142.110.239.4  HTTP        351 GET / HTTP/1.1
 105 18.890959  142.110.239.4  192.168.1.75   TCP          60 http > 46044 [ACK] Seq=1 Ack=298 Win=32471 Len=0
```

```
+ Ethernet II, Src: Vmware_d9:13:d0 (00:0c:29:d9:13:d0), Dst: Actionte_eb:cc:98 (a8:39:44:eb:cc:98)
+ Internet Protocol Version 4, Src: 192.168.1.75 (192.168.1.75), Dst: 142.110.239.4 (142.110.239.4)
+ Transmission Control Protocol, Src Port: 46044 (46044), Dst Port: http (80), Seq: 1, Ack: 1, Len: 297
- Hypertext Transfer Protocol
  + GET / HTTP/1.1\r\n
    Host: www.sait.ca\r\n
    User-Agent: Mozilla/5.0 (X11; Linux i686 on x86_64; rv:13.0) Gecko/20100101 Firefox/13.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    DNT: 1\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://www.sait.ca/]
```

```
0000  a8 39 44 eb cc 98 00 0c  29 d9 13 d0 08 00 45 00   .9D..... ).....E.
0010  01 51 8a 34 40 00 40 06  70 0c c0 a8 01 4b 8e 6e   .Q.4@.@. p....K.n
0020  ef 04 b3 dc 00 50 bf e7  7c 12 02 4a 24 f1 50 18   .....P.. |..J$.P.
0030  39 08 12 4d 00 00 47 45  54 20 2f 20 48 54 54 50   9..M..GE T / HTTP
0040  2f 31 2e 31 0d 0a 48 6f  73 74 3a 20 77 77 77 2e   /1.1..Ho st: www.
0050  73 61 69 74 2e 63 61 0d  0a 55 73 65 72 2d 41 67   sait.ca. .User-Ag
0060  65 6e 74 3a 20 4d 6f 7a  69 6c 6c 61 2f 35 2e 30   ent: Moz illa/5.0
0070  20 28 58 31 31 3b 20 4c  69 6e 75 78 20 69 36 38    (X11; L inux i68
0080  36 20 6f 6e 20 78 38 36  5f 36 34 3b 20 72 76 3a   6 on x86 _64; rv:
0090  31 33 2e 30 29 20 47 65  63 6b 6f 2f 32 30 31 30   13.0) Ge cko/2010
00a0  30 31 30 31 20 46 69 72  65 66 6f 78 2f 31 33 2e   0101 Fir efox/13.
```

File: "/tmp/wireshark_eth2_2013010€ Packets: 935 Displayed: 935 Marked: 0 Dropped: 133 Profile: Default

HTTP - URLs

- URL
  - Uniform Resource Locator:
    - protocol (http, ftp)
    - host name (name.domain name)
    - port (usually 80 but many on 8080)
    - directory path to the resource
    - resource name
  - http://xxx.mydomain.ca/www/index.html.

State and Sessions

Techniques

- URL rewriting
- Hidden form fields
- Cookies
- SSL sessions

Statelessness

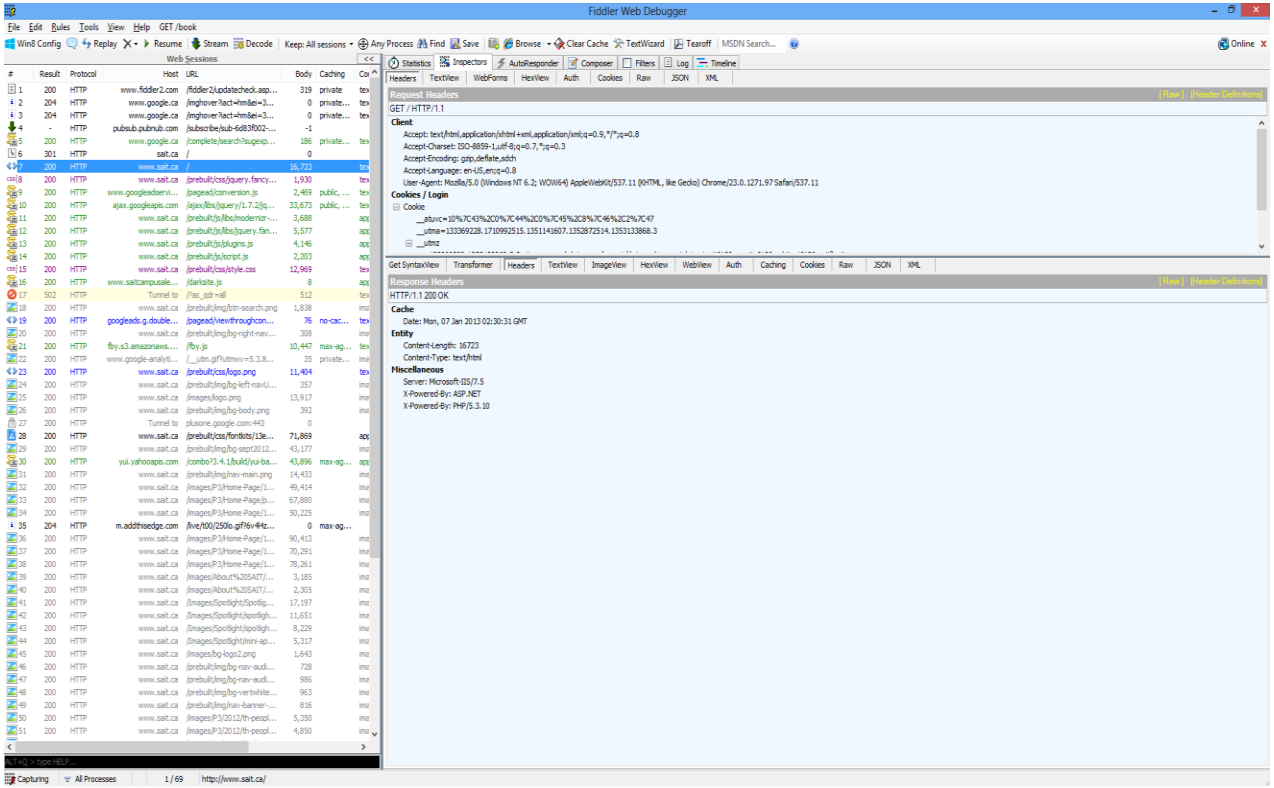
- Because of the Connect, Request, Response, Disconnect nature of HTTP it is said to be a stateless protocol
  - i.e. from one web page to the next there is nothing in the protocol that allows a web program to maintain program “state” (like a desktop program).
  - “state” can be maintained by “witchery” or “trickery” if it is needed

Cookies

- Extension of HTTP that allows servers to store data on the clients;
- Limited size and number;
- May be disabled by the client;
- Set-Cookie: sessionid=21A9A8089C305319; path=/
- Cookie: sessionid=21A9A8089C305319

Useful Tools

Fiddler: It is a Web Debugging Proxy which logs all HTTP(S) traffic between your computer and the Internet.


Fiddler Web Debugger
File Edit Rules Tools View Help GET /book
Win8 Config Replay Resume Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard Tearoff MSDN Search... Online
Web Sessions
Statistics Inspectors AutoResponder Composer Filters Log Timeline
Headers TextView WebForms HexView Auth Cookies Raw JSON XML
Get SyntaxView Transformer Headers TextView ImageView HexView WebView Auth Caching Cookies Raw JSON XML
[Raw] [Header Definitions]

#	Result	Protocol	Host	URL	Body	Caching	Co
1	200	HTTP	www.fiddler2.com	/fiddler2/updatecheck.asp...	319	private	tex
2	204	HTTP	www.google.ca	/imghover?iact=hm&ei=3...	0	private...	tex
3	204	HTTP	www.google.ca	/imghover?iact=hm&ei=3...	0	private...	tex
4	-	HTTP	pubsub.pubnub.com	/subscribe/sub-6d83f002-...	-1		
5	200	HTTP	www.google.ca	/complete/search?sugexp...	186	private...	tex
6	301	HTTP	sait.ca	/	0		
7	200	HTTP	www.sait.ca	/	16,723		tex
8	200	HTTP	www.sait.ca	/prebuilt/css/jquery.fancy...	1,930		tex
9	200	HTTP	www.googleadservi...	/pagead/conversion.js	2,469	public, ...	tex
10	200	HTTP	ajax.googleapis.com	/ajax/libs/jquery/1.7.2/jq...	33,673	public, ...	tex
11	200	HTTP	www.sait.ca	/prebuilt/js/libs/modernizr-...	3,688		app
12	200	HTTP	www.sait.ca	/prebuilt/js/libs/jquery.fan...	5,577		app
13	200	HTTP	www.sait.ca	/prebuilt/js/plugins.js	4,146		app
14	200	HTTP	www.sait.ca	/prebuilt/js/script.js	2,203		app
15	200	HTTP	www.sait.ca	/prebuilt/css/style.css	12,969		tex
16	200	HTTP	www.saitcampusale...	/darksite.js	8		app
17	502	HTTP	Tunnel to	/?as_qdr=all	512		tex
18	200	HTTP	www.sait.ca	/prebuilt/img/btn-search.png	1,838		ima
19	200	HTTP	googleads.g.double...	/pagead/viewthroughcon...	76	no-cac...	tex
20	200	HTTP	www.sait.ca	/prebuilt/img/bg-right-nav...	308		ima
21	200	HTTP	fby.s3.amazonaws....	/fby.js	10,447	max-ag...	tex
22	200	HTTP	www.google-analyti...	/__utm.gif?utmwv=5.3.8...	35	private...	ima
23	200	HTTP	www.sait.ca	/prebuilt/css/logo.png	11,404		tex
24	200	HTTP	www.sait.ca	/prebuilt/img/bg-left-navU...	357		ima
25	200	HTTP	www.sait.ca	/images/logo.png	13,917		ima
26	200	HTTP	www.sait.ca	/prebuilt/img/bg-body.png	392		ima
27	200	HTTP	Tunnel to	plusone.google.com:443	0		
28	200	HTTP	www.sait.ca	/prebuilt/css/fontkits/13e...	71,869		app
29	200	HTTP	www.sait.ca	/prebuilt/img/bg-sept2012...	43,177		ima
30	200	HTTP	yui.yahooapis.com	/combo?3.4.1/build/yui-ba...	43,896	max-ag...	app
31	200	HTTP	www.sait.ca	/prebuilt/img/nav-main.png	14,433		ima
32	200	HTTP	www.sait.ca	/images/P3/Home-Page/1...	49,414		ima
33	200	HTTP	www.sait.ca	/images/P3/Home-Page/p...	67,880		ima
34	200	HTTP	www.sait.ca	/images/P3/Home-Page/1...	50,225		ima
35	204	HTTP	m.addthisedge.com	/live/t00/250lo.gif?6v4l4z...	0	max-ag...	
36	200	HTTP	www.sait.ca	/images/P3/Home-Page/1...	90,413		ima
37	200	HTTP	www.sait.ca	/images/P3/Home-Page/1...	70,291		ima
38	200	HTTP	www.sait.ca	/images/P3/Home-Page/1...	78,261		ima
39	200	HTTP	www.sait.ca	/images/About%20SAIT/...	3,185		ima
40	200	HTTP	www.sait.ca	/images/About%20SAIT/...	2,305		ima
41	200	HTTP	www.sait.ca	/Images/Spotlight/Spotlig...	17,197		ima
42	200	HTTP	www.sait.ca	/Images/Spotlight/spotligh...	11,651		ima
43	200	HTTP	www.sait.ca	/Images/Spotlight/spotligh...	8,229		ima
44	200	HTTP	www.sait.ca	/Images/Spotlight/mini-ap...	5,317		ima
45	200	HTTP	www.sait.ca	/images/bg-logo2.png	1,643		ima
46	200	HTTP	www.sait.ca	/prebuilt/img/bg-nav-audi...	728		ima
47	200	HTTP	www.sait.ca	/prebuilt/img/bg-nav-audi...	986		ima
48	200	HTTP	www.sait.ca	/prebuilt/img/bg-vertwhite...	963		ima
49	200	HTTP	www.sait.ca	/prebuilt/img/nav-banner-...	816		ima
50	200	HTTP	www.sait.ca	/images/P3/2012/th-peopl...	5,350		ima
51	200	HTTP	www.sait.ca	/images/P3/2012/th-peopl...	4,850		ima

ALT+Q > type HELP...

Capturing | All Processes | 1 / 69 | http://www.sait.ca/

Request Headers

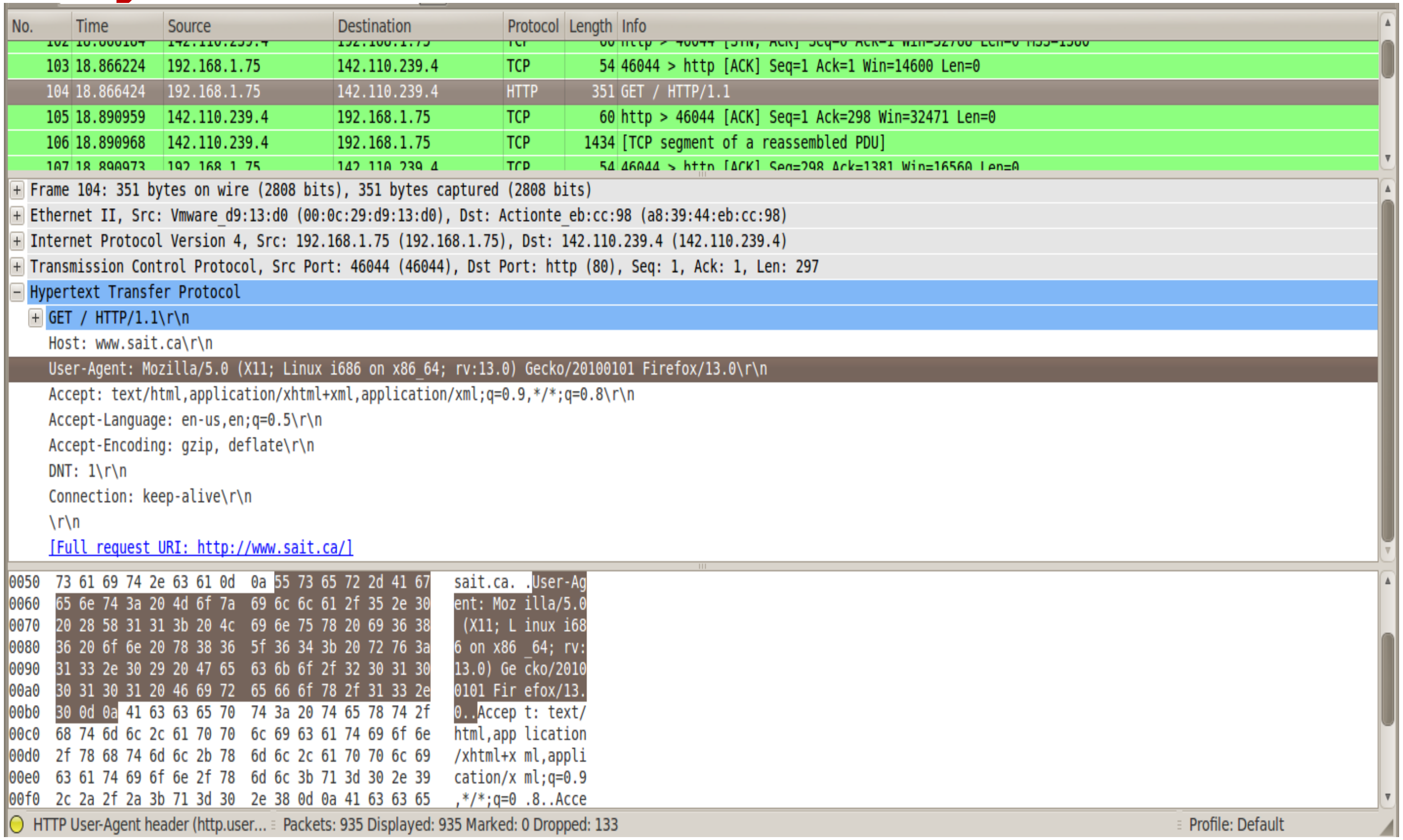
```
GET / HTTP/1.1
Client
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
    Accept-Encoding: gzip,deflate,sdch
    Accept-Language: en-US,en;q=0.8
    User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.11 (KHTML, like Gecko) Chrome/23.0.1271.97 Safari/537.11
Cookies / Login
  ⊟ Cookie
        __atuvc=10%7C43%2C0%7C44%2C0%7C45%2C8%7C46%2C2%7C47
        __utma=133369228.1710992515.1351141607.1352872514.1353133868.3
      ⊟ __utmz
```

Response Headers

```
HTTP/1.1 200 OK
Cache
    Date: Mon, 07 Jan 2013 02:30:31 GMT
Entity
    Content-Length: 16723
    Content-Type: text/html
Miscellaneous
    Server: Microsoft-IIS/7.5
    X-Powered-By: ASP.NET
    X-Powered-By: PHP/5.3.10
```

Useful Tools

Wireshark: It is a network protocol analyzer for Unix and Windows



```
No.    Time       Source          Destination     Protocol Length Info
   102 18.866104  142.110.239.4   192.168.1.75    TCP          60 http > 46044 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1380
   103 18.866224  192.168.1.75    142.110.239.4   TCP          54 46044 > http [ACK] Seq=1 Ack=1 Win=14600 Len=0
   104 18.866424  192.168.1.75    142.110.239.4   HTTP        351 GET / HTTP/1.1
   105 18.890959  142.110.239.4   192.168.1.75    TCP          60 http > 46044 [ACK] Seq=1 Ack=298 Win=32471 Len=0
   106 18.890968  142.110.239.4   192.168.1.75    TCP        1434 [TCP segment of a reassembled PDU]
   107 18.890973  192.168.1.75    142.110.239.4   TCP          54 46044 > http [ACK] Seq=298 Ack=1381 Win=16560 Len=0
```

```
+ Frame 104: 351 bytes on wire (2808 bits), 351 bytes captured (2808 bits)
+ Ethernet II, Src: Vmware_d9:13:d0 (00:0c:29:d9:13:d0), Dst: Actionte_eb:cc:98 (a8:39:44:eb:cc:98)
+ Internet Protocol Version 4, Src: 192.168.1.75 (192.168.1.75), Dst: 142.110.239.4 (142.110.239.4)
+ Transmission Control Protocol, Src Port: 46044 (46044), Dst Port: http (80), Seq: 1, Ack: 1, Len: 297
- Hypertext Transfer Protocol
  + GET / HTTP/1.1\r\n
    Host: www.sait.ca\r\n
    User-Agent: Mozilla/5.0 (X11; Linux i686 on x86_64; rv:13.0) Gecko/20100101 Firefox/13.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    DNT: 1\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://www.sait.ca/]
```

```
0050  73 61 69 74 2e 63 61 0d  0a 55 73 65 72 2d 41 67   sait.ca. .User-Ag
0060  65 6e 74 3a 20 4d 6f 7a  69 6c 6c 61 2f 35 2e 30   ent: Moz illa/5.0
0070  20 28 58 31 31 3b 20 4c  69 6e 75 78 20 69 36 38    (X11; L inux i68
0080  36 20 6f 6e 20 78 38 36  5f 36 34 3b 20 72 76 3a   6 on x86 _64; rv:
0090  31 33 2e 30 29 20 47 65  63 6b 6f 2f 32 30 31 30   13.0) Ge cko/2010
00a0  30 31 30 31 20 46 69 72  65 66 6f 78 2f 31 33 2e   0101 Fir efox/13.
00b0  30 0d 0a 41 63 63 65 70  74 3a 20 74 65 78 74 2f   0..Accep t: text/
00c0  68 74 6d 6c 2c 61 70 70  6c 69 63 61 74 69 6f 6e   html,app lication
00d0  2f 78 68 74 6d 6c 2b 78  6d 6c 2c 61 70 70 6c 69   /xhtml+x ml,appli
00e0  63 61 74 69 6f 6e 2f 78  6d 6c 3b 71 3d 30 2e 39   cation/x ml;q=0.9
00f0  2c 2a 2f 2a 3b 71 3d 30  2e 38 0d 0a 41 63 63 65   ,*/*;q=0 .8..Acce
```

```
○ HTTP User-Agent header (http.user... Packets: 935 Displayed: 935 Marked: 0 Dropped: 133    Profile: Default
```

Information Gathering - Tools

Target discovery

genlist: tool can be used to get a list of hosts that respond to the ping probes (ping scanner).

Syntax

#genlist IP_Information

```
EXAMPLE
[root@sait tmp]# genlist –s 192.168.1.\*
192.168.1.64
192.168.1.65
192.168.1.66
192.168.1.69
```

Information Gathering - Tools

Target discovery

nping: Network packet generation tool (TCP, UDP, ICMP, ARP) / ping utility.

Syntax

#nping [options] IP_Address

```
EXAMPLE
[root@sait tmp]#   nping -c 1 --tcp -p 80 --flags syn 10.2.2.1
SENT (0.0031s) TCP 10.2.2.30:14988 > 10.2.2.1:80 S ttl=64 id=3213 iplen=40
seq=1836200572 win=1480
RCVD (0.0038s) TCP 10.2.2.1:80 > 10.2.2.30:14988 SA ttl=64 id=0 iplen=44
seq=3156447310 win=5840 <mss 1460>
nping_event_handler(): TIMER killed: Resource temporarily unavailable
```

Note: S = SYN and SA = SYN-ACK, the target has port 80 open.

> Backtrack | Information Gathering | Network Analysis | Identify Live Hosts

Information Gathering - Tools

Target discovery

nping: Network packet generation tool (TCP, UDP, ICMP, ARP) / ping utility.

Syntax

#nping [options] IP_Address

EXAMPLE

```
[root@sait tmp]#   nping -c 1 --tcp -p 8080 --flags syn 10.2.2.1
SENT (0.0041s) TCP 10.2.2.30:13280 > 10.2.2.1:8080 S ttl=64 id=3773 iplen=40 seq=1614043183 win=1480
RCVD (0.0047s) TCP 10.2.2.1:8080 > 10.2.2.30:13280 RA ttl=64 id=0 iplen=40  seq=0 win=0
```

Note: S = SYN and RA = RST-ACK, it does not have port 8080 open.

> Backtrack | Information Gathering | Network Analysis | Identify Live Hosts

Information Gathering - Tools

Service Enumeration

AMAP: it can be used to check the application that is running on a specific port (Application Map).

Syntax

#amap [options] IP_Address Port

```
EXAMPLE
[root@sait tmp]#    amap -bq 10.2.2.1 80
/>\n</p>\n<hr>\n<address>Apache/2.2.8 (Ubuntu)
Protocol on 10.2.2.1:80/tcp matches http-apache-2 - banner: <!DOCTYPE HTML
PUBLIC "-//IETF//DTD HTML 2.0//EN">\n<html><head>\n<title>400 Bad
Request</title>\n</head><body>\n<h1>Bad Request</h1>\n<p>Your browser sent a
request that this server could not understand.<br
/>\n</p>\n<hr>\n<address>Apache/2.2.8 (Ubuntu)
```

> Backtrack | Information Gathering | Network Analysis | Service Fingerprinting

Information Gathering - Tools

Service Enumeration

HTTPRINT: it can be used to detect an HTTP service software and version (web server fingerprinting tool).

Syntax

```
#httprint [options] IP_Address –s signatures.txt
```

```
EXAMPLE
root@bt:/pentest/enumeration/web/httprint/linux# ./httprint -h 10.2.2.1 -s signatures.txt
Finger Printing on http://10.2.2.1:80/
Finger Printing Completed on http://10.2.2.1:80/
--------------------------------------------------
Host: 10.2.2.1
Derived Signature:
Apache/2.2.8 (Ubuntu) DAV/2
```

> Backtrack | Information Gathering | Network Analysis | Service Fingerprinting

Information Gathering - Tools

Service Enumeration

HTTSQUASH: it can be used to detect an HTTP service software and version.

Syntax

#httsquash [options] IP_Address

```
EXAMPLE
root@bt:/pentest/scanners/httsquash# ./httsquash -r 10.2.2.1
FOUND: 10.2.2.1 80
HTTP/1.1 200 OK
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Content-Type: text/html
```

> Backtrack | Information Gathering | Network Analysis | Service Fingerprinting

Mapping - Tools

NMAP: Most powerful and preferred port scanner for security professionals.

Scan Option	Name	Notes	Example
-sS	TCP SYN	Stealth scan. The full TCP connection is not established	#nmap –sS 192.168.1.0/24
-sT	TCP Full	Full connect. Most detectable	#nmap –sT 192.168.1.0/24
-sU	UDP	UDP scanning	#nmap –sU 192.168.1.0/24
-sP	Ping	Performs a ping sweep	#nmap –sP 192.168.1.0/24
-P0	Don't ping	Perform the scan even the target doesn't not respond to ping	#nmap –P0 192.168.1.0/24
-T<0-5>	Time	Set the timing template (higher is faster)	#nmap –O –T5 192.168.1.0/24
-p0-65535	TCP scan	It will scan all the 65,536 ports	#nmap –sS –p0-65535 192.168.1.1
-p22	Port	Port specification	#nmap –O –p22 192.168.1.1

Mapping – Tools

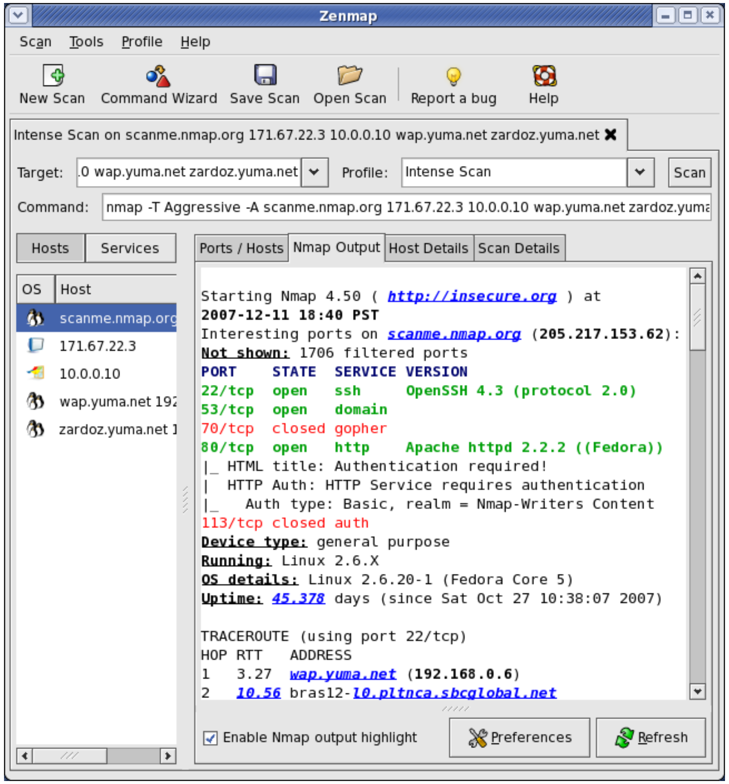
NMAP: Most powerful and preferred port scanner for security professionals.

Scan Option	Name	Notes	Example
-sS	TCP SYN	Stealth scan. Called half opened scan because it never completes a connection with the target.	#nmap –sS 192.168.1.0/24
-sV	Service	Service detection	#nmap –sV –O 192.168.1.1
-O	OS Fingerprinting	It will try to find the OS running on the machine	#nmap –O 192.168.1.1
-sA	ACK scan	Shows which port is filtered or unfiltered by the Firewall	#nmap –sA 10.2.2.1
-D	Decoy	Shows that the scan attempt is coming from different sources.	#nmap –sS 10.2.2.1 –D 192.168.10.1,192.168.10.2,192.168.10.3
-sN	Null Scan	They are probes made with packets that violate traditional TCP connection.	#nmap –sN 10.2.2.1

Mapping – Tools

ZENMAP: it is a graphical interface of Nmap.

- Can do a comparison between scans;
- Keeps track of the scan results;
- It can even draw a topological map of the discovered network.



Intense Scan on scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma.net ✖

Target: .0 wap.yuma.net zardoz.yuma.net

Profile: Intense Scan

Command: nmap -T Aggressive -A scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma

scanme.nmap.org
171.67.22.3
10.0.0.10
wap.yuma.net 192
zardoz.yuma.net 1

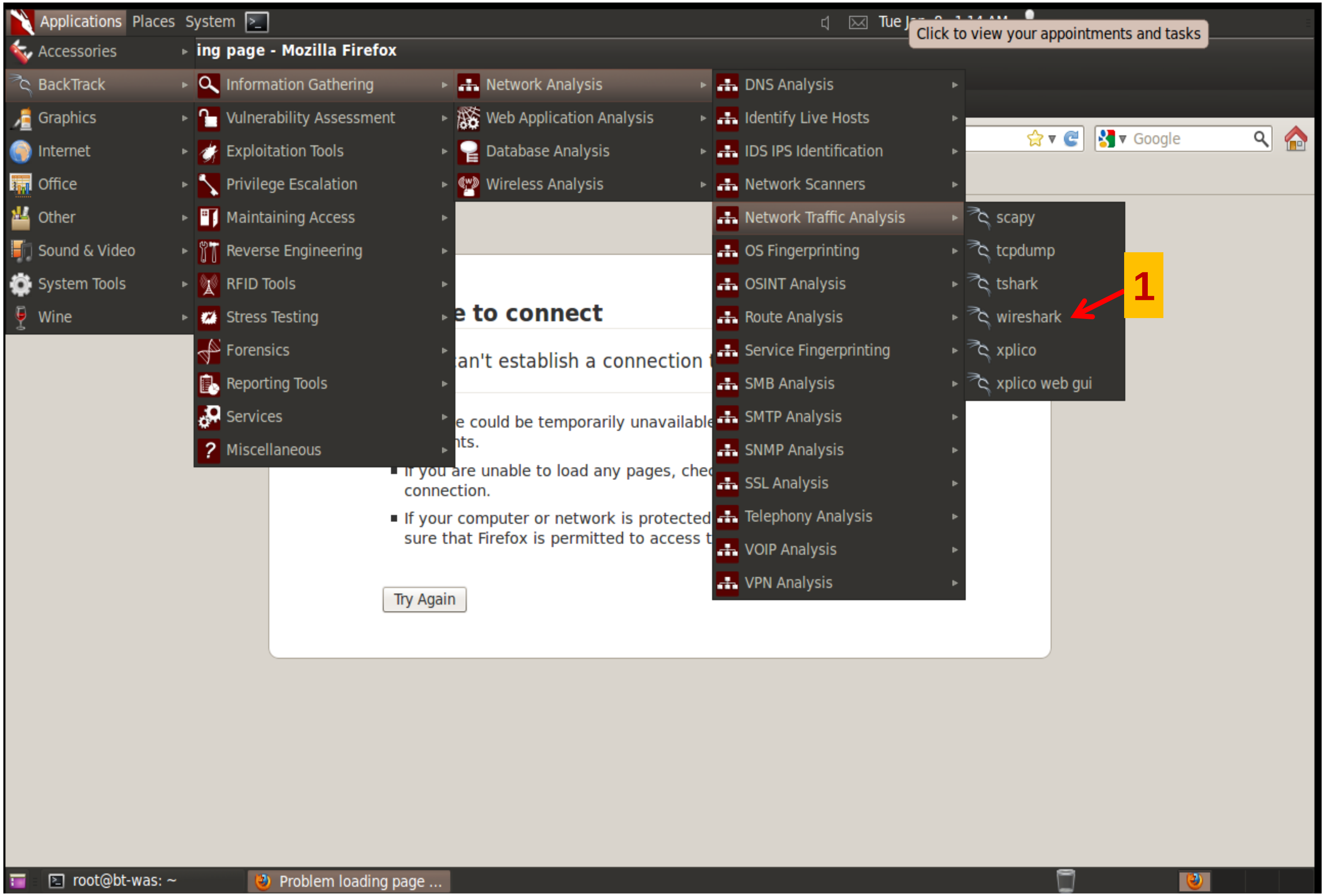
```
Starting Nmap 4.50 ( http://insecure.org ) at
2007-12-11 18:40 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
Not shown: 1706 filtered ports
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 4.3 (protocol 2.0)
53/tcp  open   domain
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.2.2 ((Fedora))
|_ HTML title: Authentication required!
|  HTTP Auth: HTTP Service requires authentication
|_   Auth type: Basic, realm = Nmap-Writers Content
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.20-1 (Fedora Core 5)
Uptime: 45.378 days (since Sat Oct 27 10:38:07 2007)

TRACEROUTE (using port 22/tcp)
HOP RTT   ADDRESS
1   3.27  wap.yuma.net (192.168.0.6)
2   10.56 bras12-10.pltnca.sbcglobal.net
```

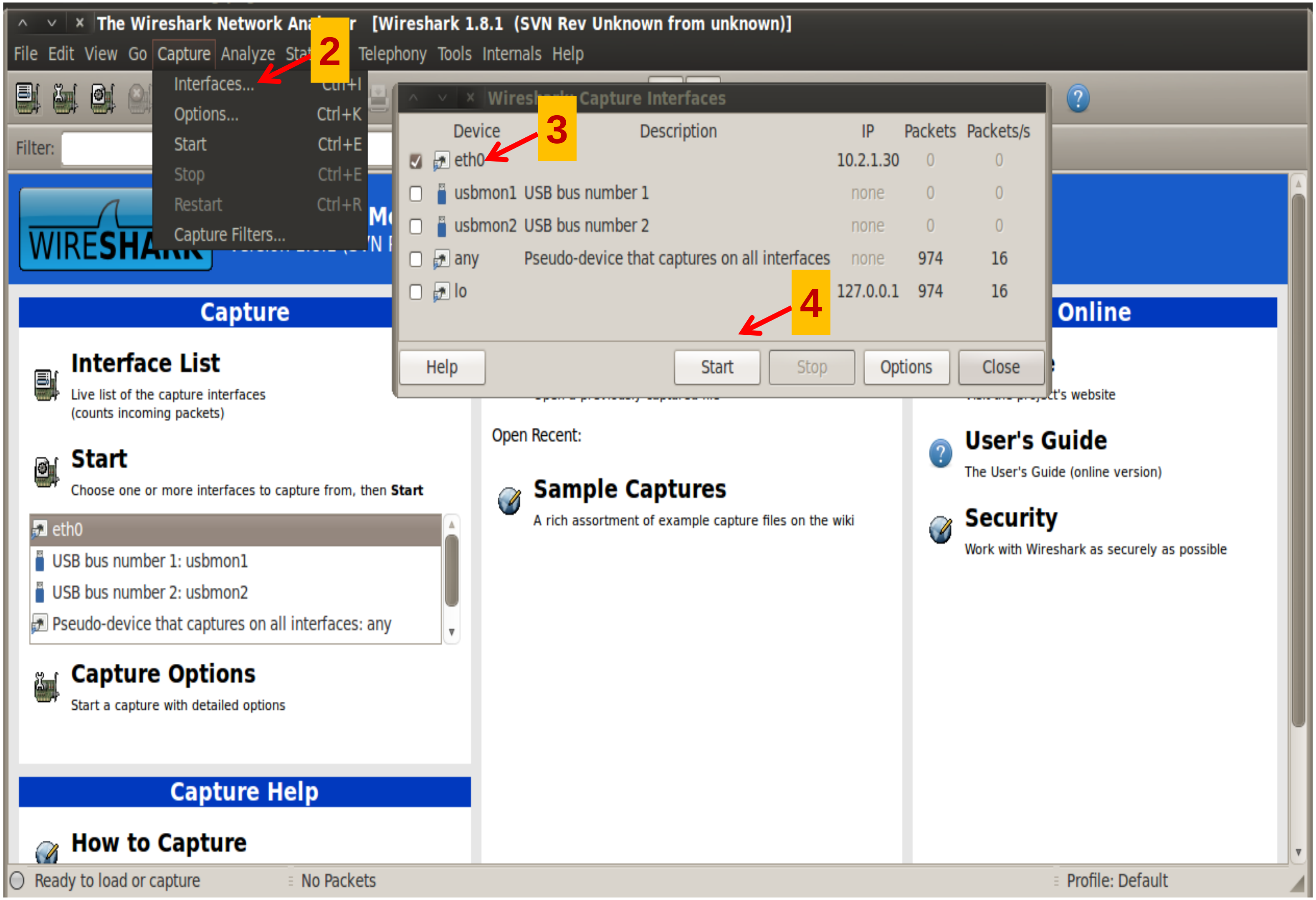
☑ Enable Nmap output highlight

> Backtrack | Information Gathering | Network Analysis | Identify Live Hosts

Lab 1 – Analyzing the HTTP Protocol



Lab 1 – Analyzing the HTTP Protocol



	Device	Description	IP	Packets	Packets/s
☑	eth0		10.2.1.30	0	0
□	usbmon1	USB bus number 1	none	0	0
□	usbmon2	USB bus number 2	none	0	0
□	any	Pseudo-device that captures on all interfaces	none	974	16
□	lo		127.0.0.1	974	16

Interface List

Live list of the capture interfaces (counts incoming packets)

Start

Choose one or more interfaces to capture from, then **Start**

- eth0
- USB bus number 1: usbmon1
- USB bus number 2: usbmon2
- Pseudo-device that captures on all interfaces: any

Capture Options

Start a capture with detailed options

How to Capture

Open Recent:

Sample Captures

A rich assortment of example capture files on the wiki

...ct's website

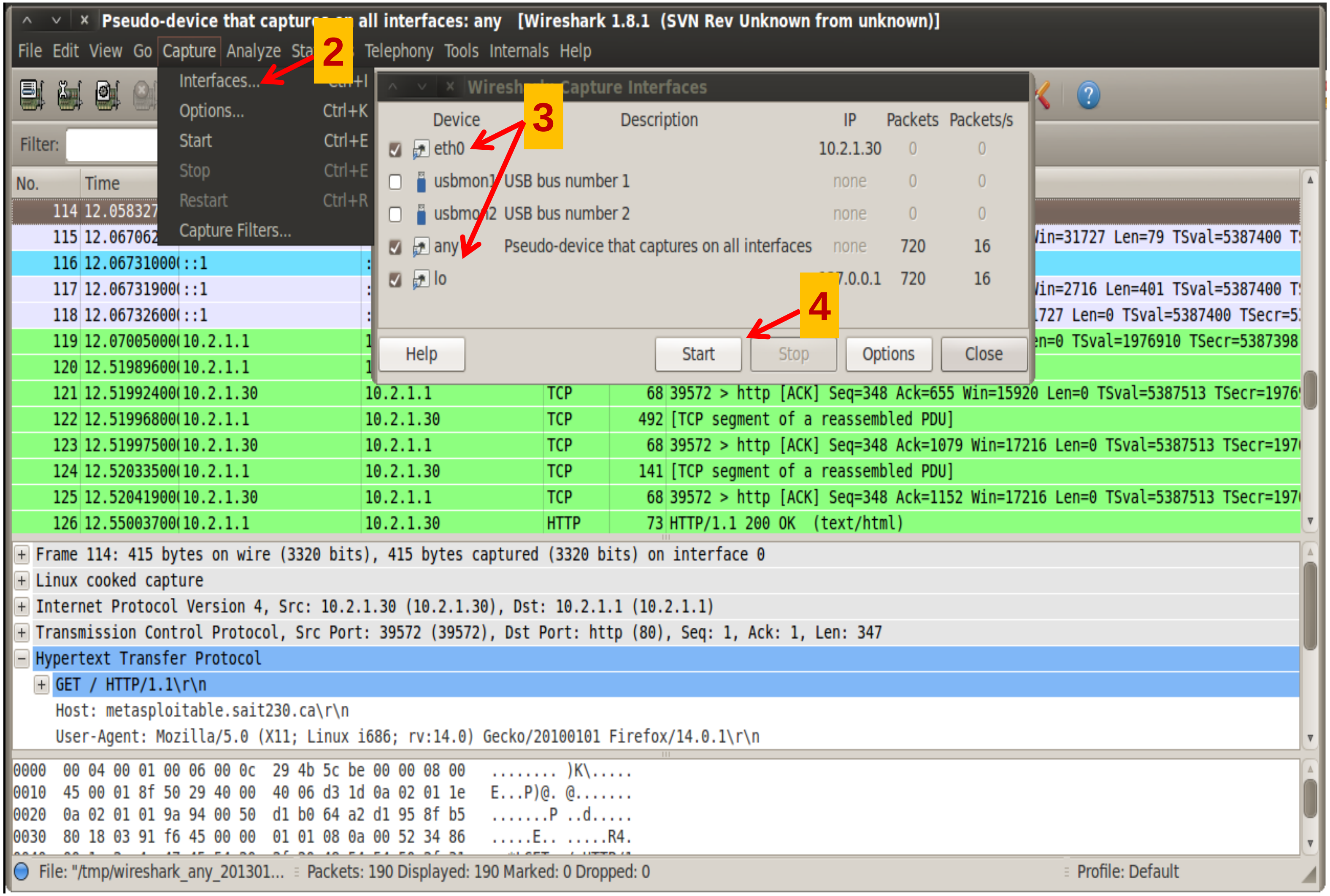
User's Guide

The User's Guide (online version)

Security

Work with Wireshark as securely as possible

Lab 1 – Analyzing the HTTP Protocol



	Device	Description	IP	Packets	Packets/s
☑	eth0		10.2.1.30	0	0
□	usbmon1	USB bus number 1	none	0	0
□	usbmon2	USB bus number 2	none	0	0
☑	any	Pseudo-device that captures on all interfaces	none	720	16
☑	lo		127.0.0.1	720	16

```
No.  Time
 114 12.058327
 115 12.067062                                                                Win=31727 Len=79 TSval=5387400 T
 116 12.06731000(::1
 117 12.06731900(::1                                                          Win=2716 Len=401 TSval=5387400 T
 118 12.06732600(::1                                                          727 Len=0 TSval=5387400 TSecr=5
 119 12.07005000(10.2.1.1                                                     en=0 TSval=1976910 TSecr=5387398
 120 12.51989600(10.2.1.1
 121 12.51992400(10.2.1.30  10.2.1.1   TCP    68 39572 > http [ACK] Seq=348 Ack=655 Win=15920 Len=0 TSval=5387513 TSecr=1976
 122 12.51996800(10.2.1.1   10.2.1.30  TCP   492 [TCP segment of a reassembled PDU]
 123 12.51997500(10.2.1.30  10.2.1.1   TCP    68 39572 > http [ACK] Seq=348 Ack=1079 Win=17216 Len=0 TSval=5387513 TSecr=197
 124 12.52033500(10.2.1.1   10.2.1.30  TCP   141 [TCP segment of a reassembled PDU]
 125 12.52041900(10.2.1.30  10.2.1.1   TCP    68 39572 > http [ACK] Seq=348 Ack=1152 Win=17216 Len=0 TSval=5387513 TSecr=197
 126 12.55003700(10.2.1.1   10.2.1.30  HTTP   73 HTTP/1.1 200 OK  (text/html)
```

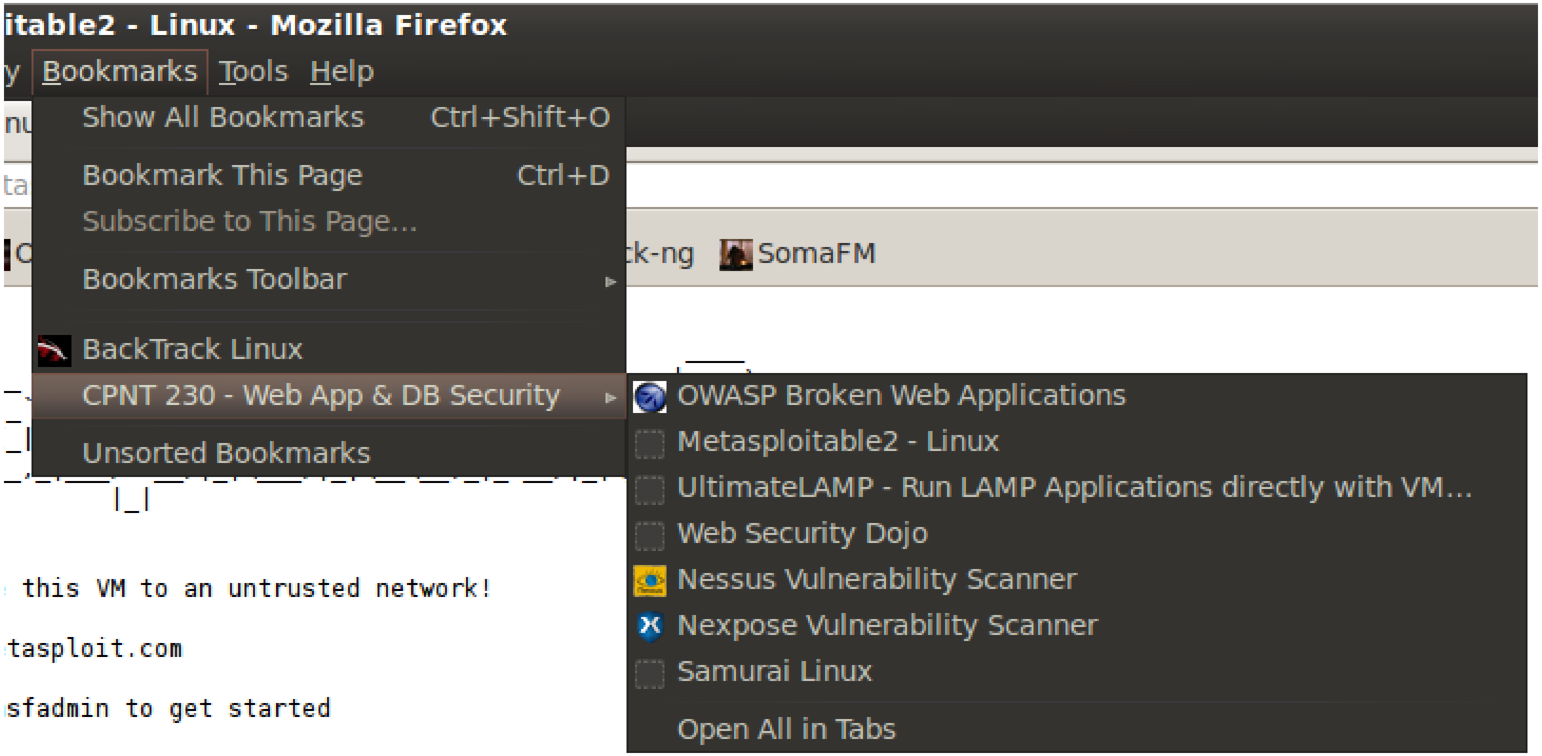
```
+ Frame 114: 415 bytes on wire (3320 bits), 415 bytes captured (3320 bits) on interface 0
+ Linux cooked capture
+ Internet Protocol Version 4, Src: 10.2.1.30 (10.2.1.30), Dst: 10.2.1.1 (10.2.1.1)
+ Transmission Control Protocol, Src Port: 39572 (39572), Dst Port: http (80), Seq: 1, Ack: 1, Len: 347
- Hypertext Transfer Protocol
  + GET / HTTP/1.1\r\n
    Host: metasploitable.sait230.ca\r\n
    User-Agent: Mozilla/5.0 (X11; Linux i686; rv:14.0) Gecko/20100101 Firefox/14.0.1\r\n
```

```
0000  00 04 00 01 00 06 00 0c  29 4b 5c be 00 00 08 00   ........ )K\.....
0010  45 00 01 8f 50 29 40 00  40 06 d3 1d 0a 02 01 1e   E...P)@. @.......
0020  0a 02 01 01 9a 94 00 50  d1 b0 64 a2 d1 95 8f b5   .......P ..d.....
0030  80 18 03 91 f6 45 00 00  01 01 08 0a 00 52 34 86   .....E.. .....R4.
```

File: "/tmp/wireshark_any_201301... Packets: 190 Displayed: 190 Marked: 0 Dropped: 0 Profile: Default

Lab 1 – Analyzing the HTTP Protocol

- Open Firefox and test the applications;
  - Metasploitable;
  - OWASP (Form).



itable2 - Linux - Mozilla Firefox

y Bookmarks Tools Help

Show All Bookmarks Ctrl+Shift+O

Bookmark This Page Ctrl+D

Subscribe to This Page...

Bookmarks Toolbar ▸

BackTrack Linux

CPNT 230 - Web App & DB Security ▸

Unsorted Bookmarks

OWASP Broken Web Applications
Metasploitable2 - Linux
UltimateLAMP - Run LAMP Applications directly with VM...
Web Security Dojo
Nessus Vulnerability Scanner
Nexpose Vulnerability Scanner
Samurai Linux
Open All in Tabs
ck-ng
SomaFM

```
 this VM to an untrusted network!

tasploit.com

sfadmin to get started
```

Lab 1 – Analyzing the HTTP Protocol

- Try to find the GET and POST request method;
- Checks for:
    - Request codes;
    - User-agent;
    - Response Status;
    - Content-length;
    - Content-Type.

Lab 2 – Gathering information about the Web Servers

- Using the following tools: Nmap, genlist, amap, nping, httpprint, httpsquash to:
  - Find the web servers available on the environment;
  - Check for application servers (usually on ports 808X, 800X);
  - Check for service version;
  - Take notes:
    - IP / Hostname;
    - Web Server / App Server;
    - Version.

Questions