

Feb 19 - 22, 2017 PHOENIX PARK, PYEONGCHANG, KOREA



# ICACT2017, 19th International Conference on Advanced Communications Technology

Technically Co-sponsored by  
the **IEEE ComSoc**



## Web Hacking & Defensing

February 19(Sun), 2017

**Prof. Thomas Byeongnam YOON, PhD.**



# Content

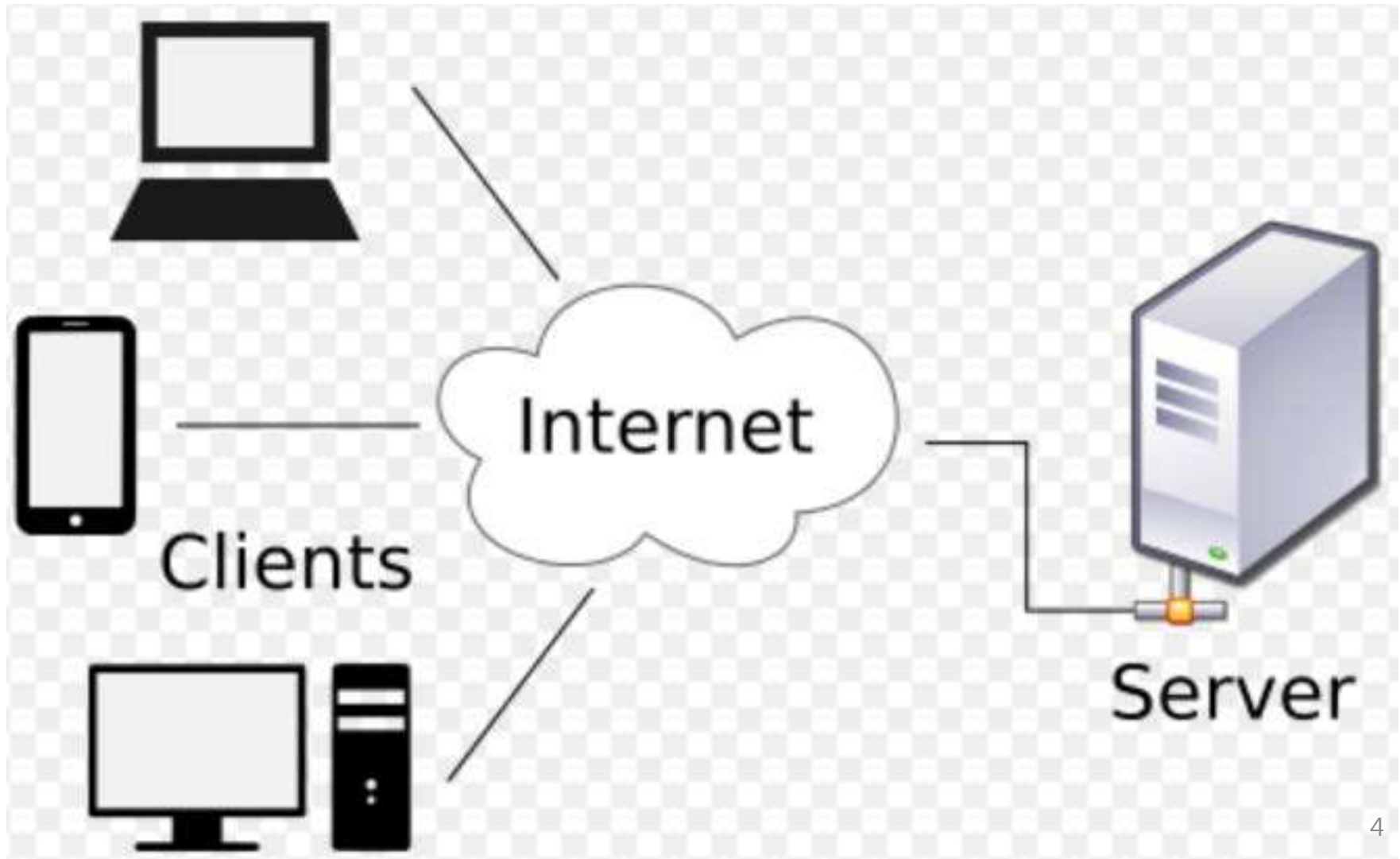
- 1. Web Protocol**
- 2. Web Log**
- 3. Web Hacking Tool**
- 4. Wrap Up**

## Learning Point : **New Terminology Definition – Clear Concept**

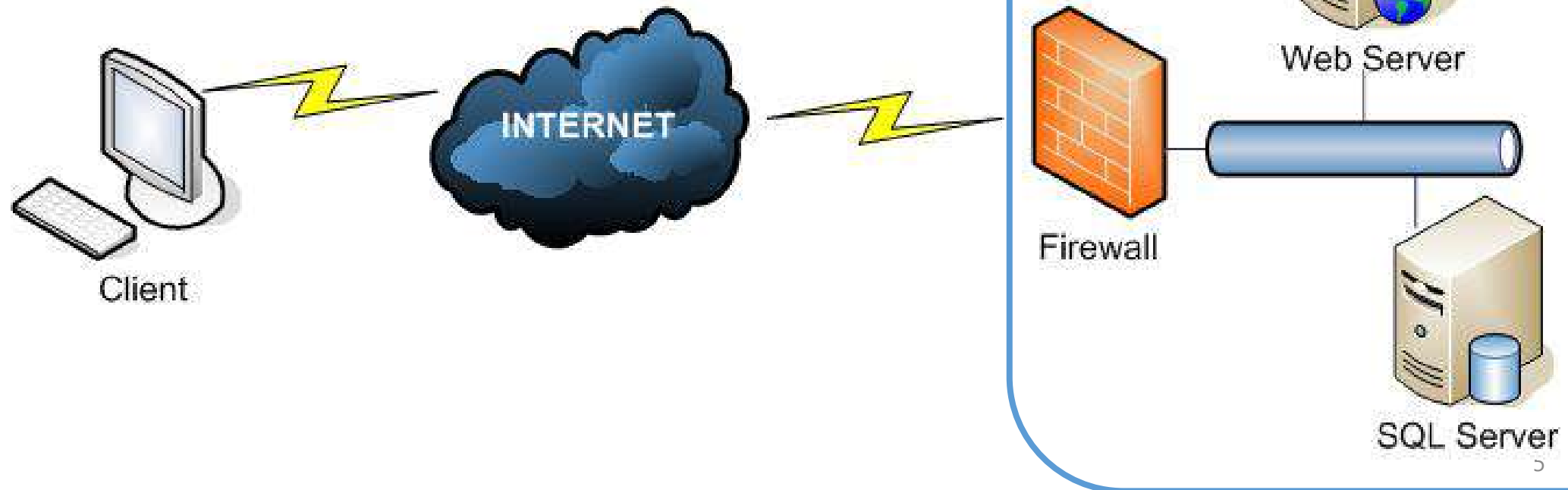
1. HTTP Protocol used for Webpages
  - **Create Cyber Space by HTML Web Program Language**
2. Paros Web Hacking Tool
  - **Strong Tool for Web Vulnerability Measure, Java Open Source Based**
3. Web Log Analysis
  - **Fundamental Knowledge of Hacking Type Analysis**
4. Web Defensing Know-How
  - **Become a Cyber Soldier – Cyber Salvation Army**



# Internet Logical Architecture → Cyber Space L.A.



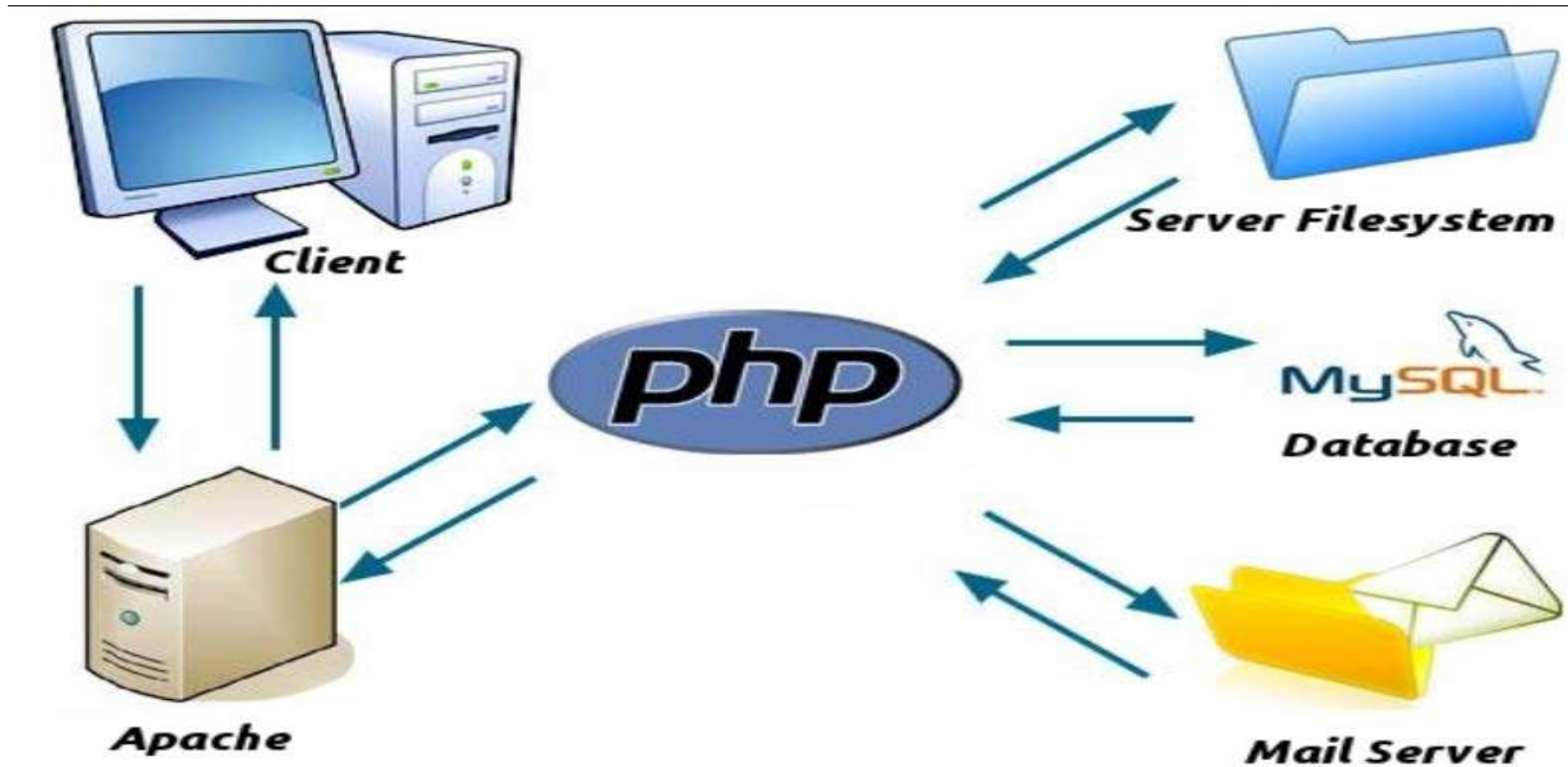
# Intranet Logical Architecture

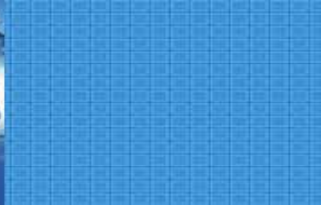




# Web Server Platform – Web Programming Environment

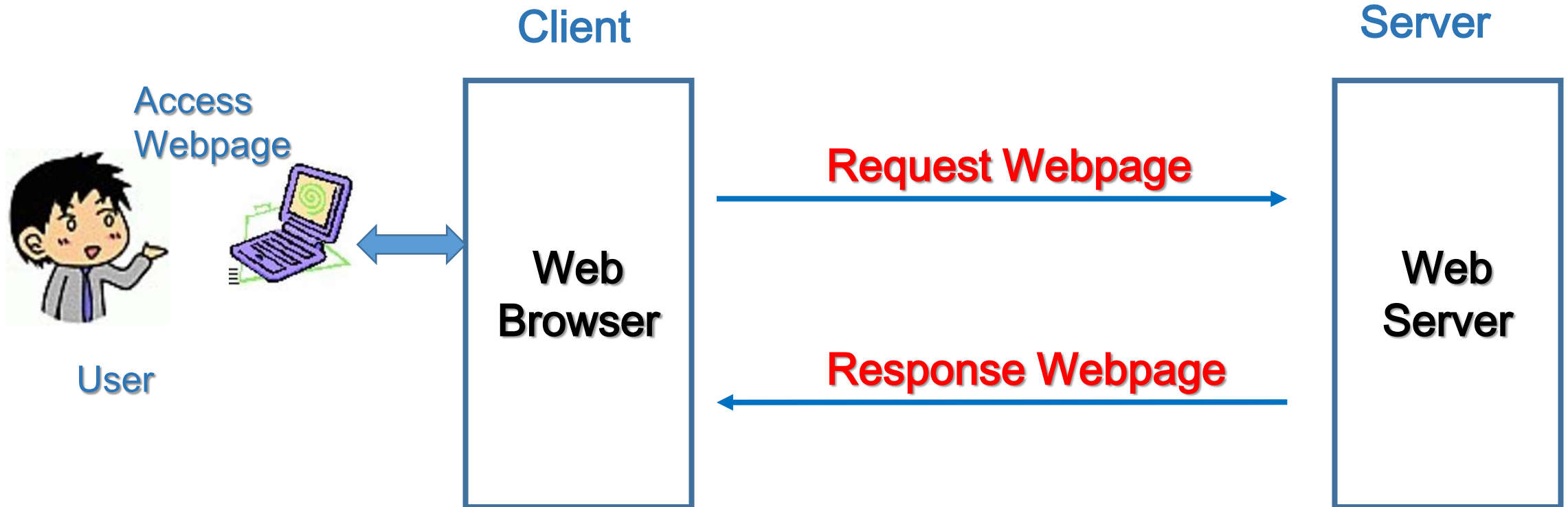
Chronicle : **HTML** + [**ASP** Platform(MS) → **JSP** Platform(Sun) → **HPH** Platform(Open Source)]





## Web Browser (UA Platform) – Cyber Space Shuttle (1993 Netscape Navigator)

Chronicle : **Netscape** (NCC) → **IE** (MS) → **Chrome** (Google: Open Source)



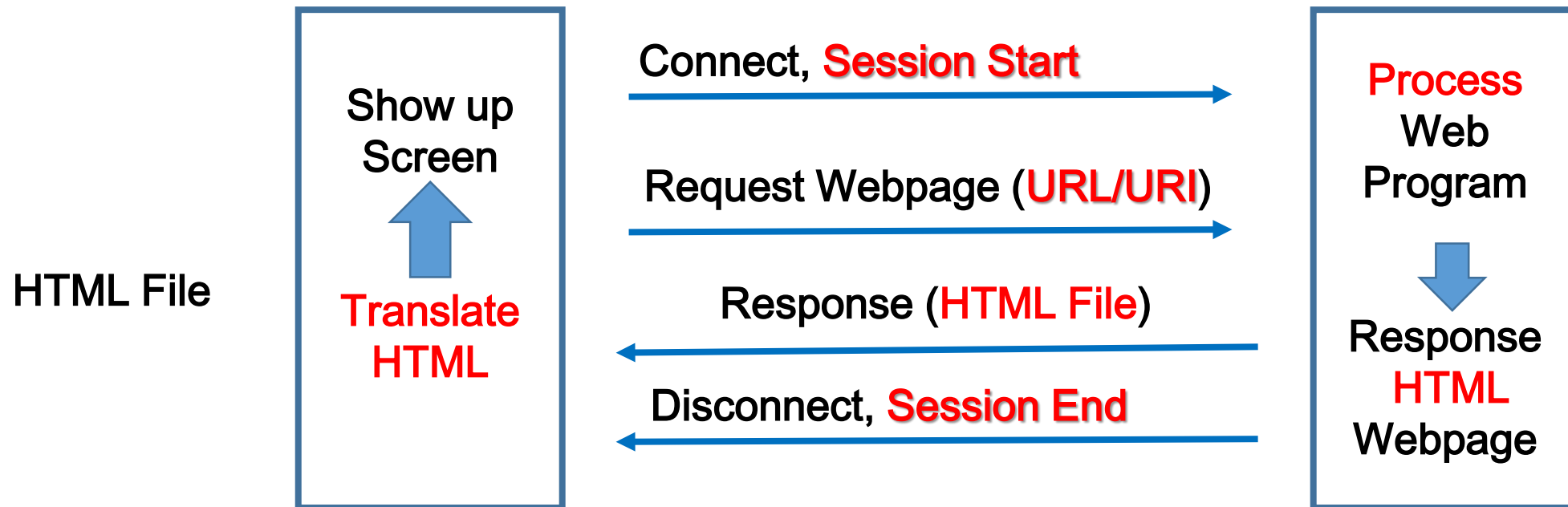
## Cyber Space Protocol – HTTP (Hyper Text Transport Protocol)

1. Web **Browser** request Webpage

2. Server Process

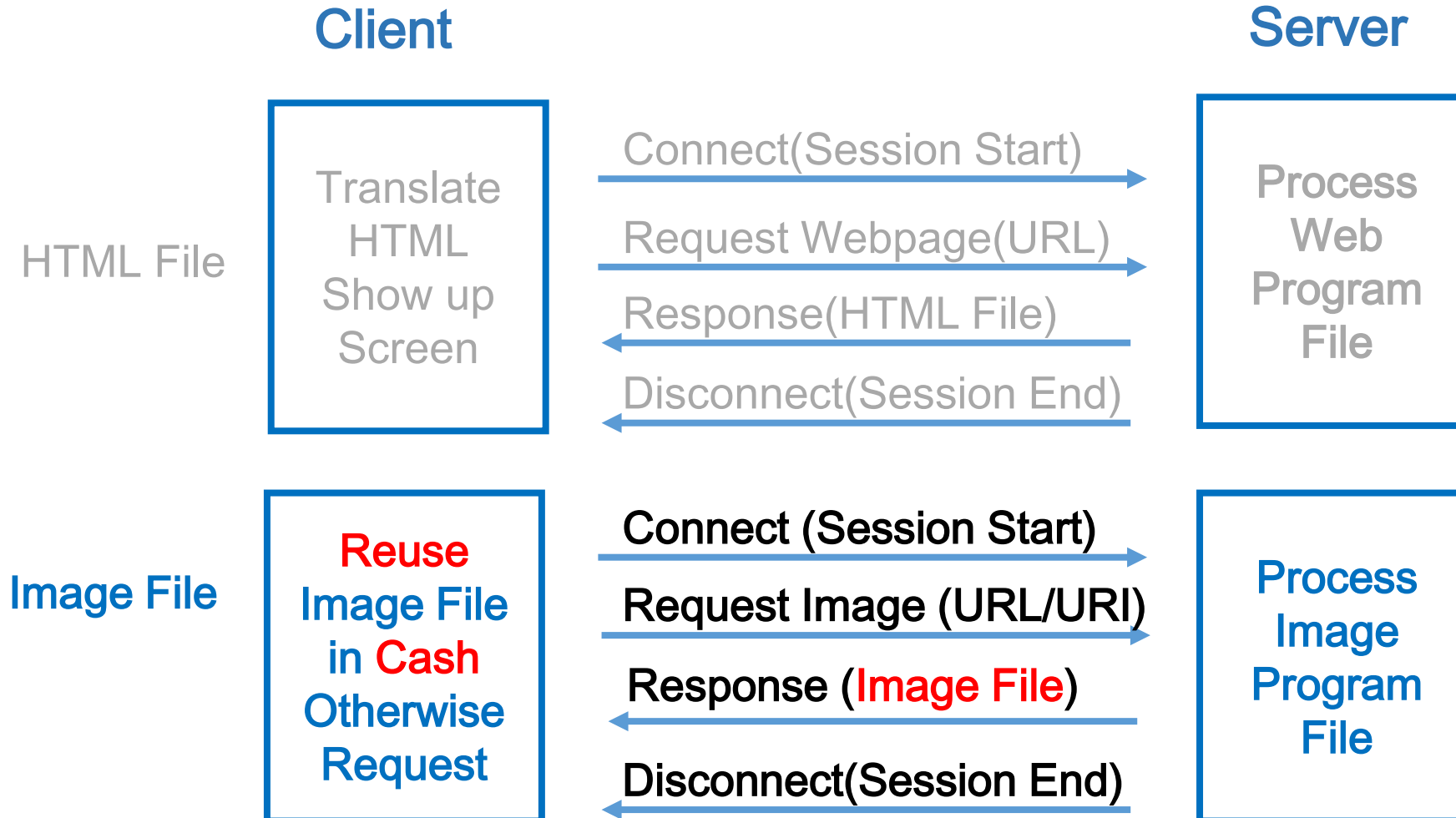
4. Execute **HTML Engine & Java Script**

3. Response Webpage





# Cyber Space Protocol – HTTP (Hyper Text Transport Protocol)





## Cyber Space Shuttle – Web Browser Doing :

### → Browser **3 Step Procedure**

**Step 1.** Session Start

**Step 2.** Data Communication

**Step 3.** Session End



Webpage

## Webpage Instances

→ **HTML5, CSS, ...**

→ Server-side Program : **ASP, JSP, PHP, ...**

→ **SQL DBMS Language**

→ **Embedded Multi-Media Languages**

: Audio, Video, Image, **Streaming Service**

: **File Upload, Download**

: Send & Receive **eMail**

: **CSV, Excel file between DBMS, ... etc.**

# Cyber Space Protocol – HTTP : Step 1. Session Start Procedure

Client



Server

Ready to Service

1. Request Connection  
(send SYN)

2. Accept Connection  
(Send SYN, ACK)

3. Confirm Connection  
(send ACK)

4. Session Start

Global Client-Server Communication Protocol



# Cyber Space Protocol – HTTP : Step 2. Data Communication Procedure

User (Browser)



Web Server

1. Request Webpage  
(HTTP method, Request  
document-PSH)

4. TCP Checksum Routine  
(send ACK)

Ready to service

2. TCP Checksum Routine  
(Send ACK)

3. Give Webpage  
(document-PSH)

4. Repeat until Completed

Global Client-Server Communication





# Cyber Space Protocol – HTTP : Step 3. Session End Procedure

User (Browser)



Web Server

1. FIN-WAIT 1  
(send FIN, ACK)  
Request Disconnection

3. FIN-WAIT 2

5. TIME WAIT  
(send ACK)

2. CLOSE-WAIT  
(send ACK)

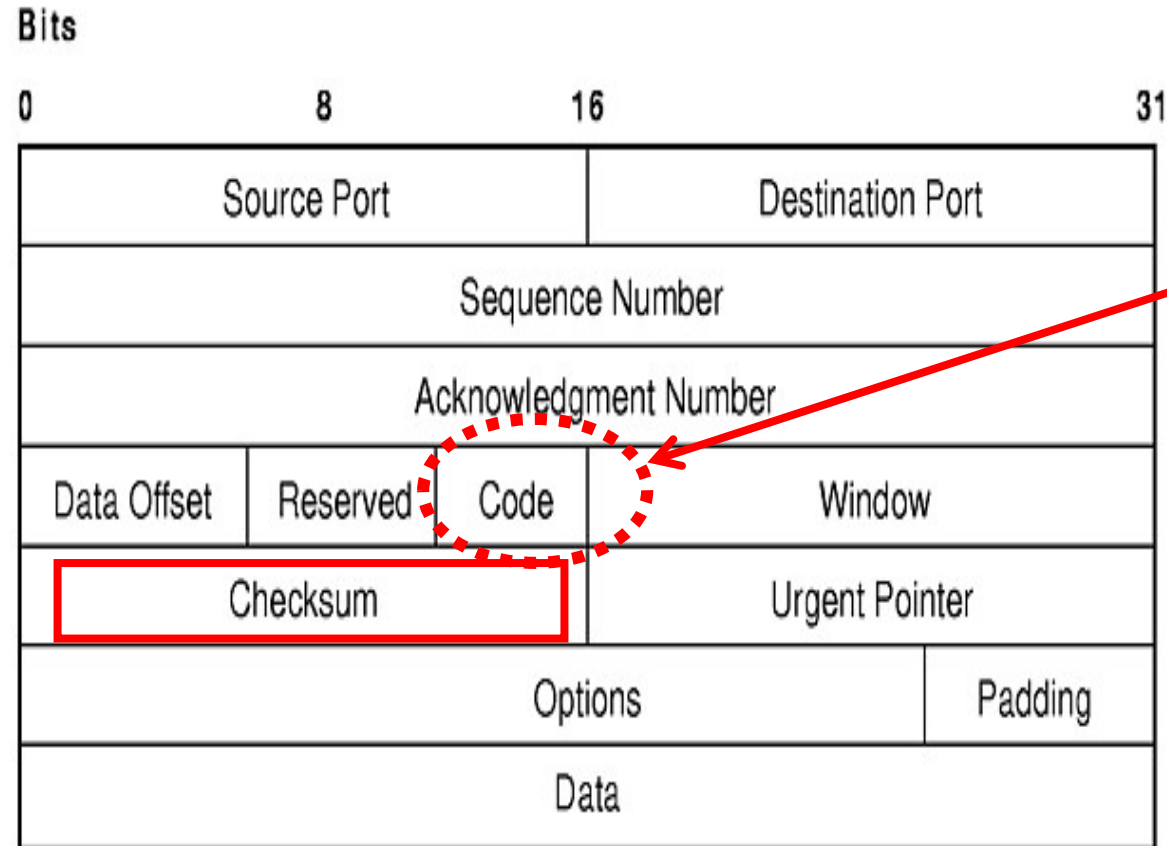
4. LAST ACK  
(Send FIN, ACK)

6. Session End

Global Client-Server Communication Protocol



# Cyber Space Protocol –TCP Date lossless Protocol Packet Format

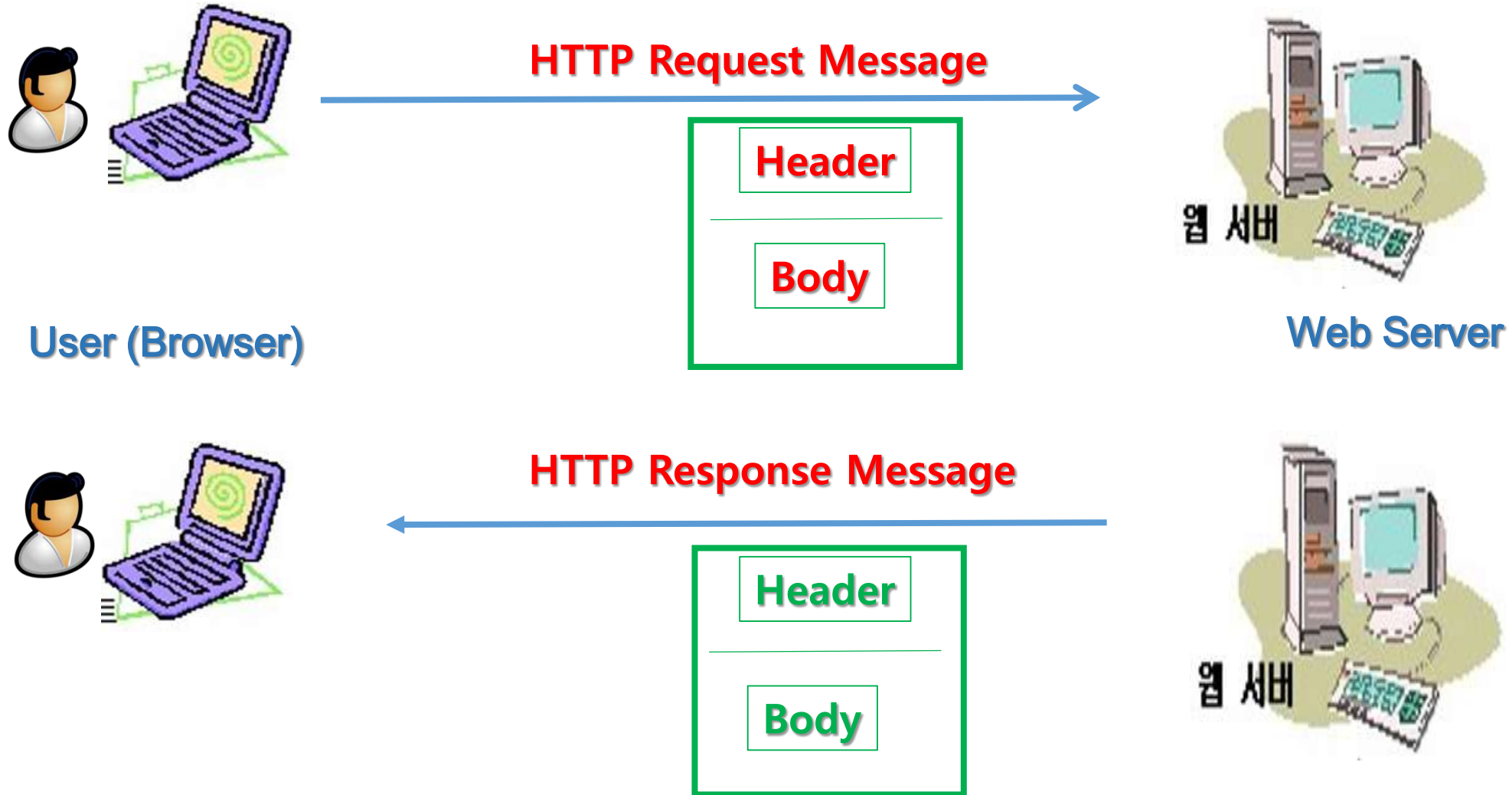


**Code - Flag Bits**  
( **Packet Control Code** )

- **URG** : Urgent Packet
- **ACK** : Acknowledgement of Message Received Well
- **PSH** : Push Request Task
- **SYN** : Data Communication Session Creation
- **FIN** : Graceful Session End Request
- **RTS** : Emergent Session End Request

Transmission Control Protocol (TCP) Packet Header

# Cyber Space Protocol – HTTP Request & Response Message Format







# Cyber Space Protocol – HTTP Request Message Format

```
GET /home/index.html HTTP/1.1
Host:www.evenstar.co.kr
Accept:text/html, text/plain
Accept-Encoding:gzip, compress
Accept-Language:ko
If-Modified-Since:Sat,31 Jan 2004 12:00:00 GMT
User-Agent:Internet Explorer6.0
```

```
-----
-----
```

본문 ( GET인 경우는 빈 공백임 )

**Header :**

HTTP Method + Host Domain +  
Client Platform Information

**White Space One Line as Separator**

**Body :**

Whole Parameters & Data





# Cyber Space Protocol – HTTP **GET Method** Request Message

- HTTP GET Method Format (**Message Header Only**)
- Message Size : **Max 2K Byte** Data Length?! ( Not enough to BBS content, etc.)

Method	Format	Description
<b>GET</b>	GET [request-uri]? <b>query_string</b> HTTP/1.1 Host:[Hostname] or [IP]	GET Method request Webpage to Server with URI(URL) in its <b>Message Header</b> Part.

<http://www.evenstar.co.kr/webpage/biglook.html> : **URL Window in Browser**

**URL/URI**(Universal Resource Identification/Location)

<http://www.evenstar.co.kr/wizboard.php?BID=notice> : Bulletin Board

**URL/URI**      **Query String**



# Cyber Space Protocol – HTTP GET Method Request Message

Request Response Trap

GET http://www.evenstar.co.kr/wizboard.php?BID=notice HTTP/1.0

← HTTP Method

Accept: \*/\*

Referer: http://www.evenstar.co.kr/webpage/top\_menu.html

Accept-Language: ko

UA-CPU: x86

Proxy-Connection: Keep-Alive

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; EmbeddedWB 14.52 from: http://www.bsalsa.com / EmbeddedWB 14.52; .NET CLR 1.1.4322; .NET CLR 2.0.50727) Paros/3.2.13

Host: www.evenstar.co.kr

Message Header Part

Message Body Part is Empty

Raw View... ▾



# Cyber Space Protocol – HTTP GET Method Request Message Scan

1. **GET** /index.html HTTP/1.1

// **Request Method**, Webpage, HTTP Version

2. **User-Agent**: MSIE 6.0; Windows NT 5.0

// User's **Web Browser**; **Platform** Version

3. **Accept**: text/html; \*/\* // Acceptable Data Type

4. **Cookie**: name = value // **User Authenticate** Information

5. **Referer**: http://www.bbb.com // **Previous passage URL**

6. **Host**: www.evenstar.co.kr // Request Domain



# Cyber Space Protocol – HTTP Post Method Request Method

- HTTP Post Method Format (**Header + Body**)  
Message Size : **No limit** ! ( Enough to BBS content, etc.)

Method	Format	Note
<b>POST</b>	POST [request-uri] HTTP/1.1 Host:[Hostname] or [IP] Content-Length:[Bytes] Content-Type:[Content Type] <hr/> <b>One White Space Line</b> <hr/> <b>[query-string] or [Data]</b>	1. Data Communication of <b>Form Based Web Page</b> with Various Data & Parameters. 2. Browser <b>can't show up it</b> at URL Window!

○ <http://www.evenstar.co.kr/wizboard.php>  
URI

**BID=notice Query String**

( http Header)

( http Body )



## Form based Webpage

icact.org/papersubmission/paper\_update.asp

Paper Information	
* Title of Paper	Experimental Validation of Multipoint Joint Processing of Range Me
* Keyword	Analytical model, Distance measurement, Radar signal processing,
* Topics	Wireless Communication
* Upload File	<input type="button" value="Choose File"/> No file chosen <span style="color: red;">PDF file only!</span> <span style="color: blue;">20170442 Paper.pdf</span> <--- <span style="color: red;">Please confirm your latest upload file</span> Do you want to upload your file? <input type="radio"/> Yes <input checked="" type="radio"/> No <input type="radio"/> Abstract(1 page) <input checked="" type="radio"/> Full Paper(Min,3 pages)
* Number of Pages	11 ▼
* E-mail(One address only)	grihafokin@gmail.com



# Cyber Space Protocol – HTTP Post Method Request Message Scan

Request Response Trap

**HTTP Method**  
POST http://www.evenstar.co.kr/wizboard/admin\_log\_check.php HTTP/1.0

**Header Part**  
Accept: /\*/\*  
Referer: http://www.evenstar.co.kr/wizboard.php?mode=login&BID=news&category=&nmode=write&UID=&CURRENT\_PAGE=  
Accept-Language: ko  
Content-Type: application/x-www-form-urlencoded  
UA-CPU: x86  
Proxy-Connection: Keep-Alive  
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; EmbeddedWB 14.52 from: http://www.bsalsa.com / EmbeddedWB 14.52; .NET CLR 1.1.4322; .NET CLR 2.0.50727) Paros/3.2.13

**Body Part**  
BID=news&Mode=MemberLogin&category=&UID=&mode=login&nmode=write&CURRENT\_PAGE=&MEMBERPASS=PASSWORD

Raw View...



# Form based Webpage HTTP Post Method Request Message Scan

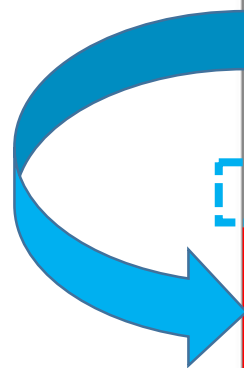
Request	Response	Trap
<pre>POST http://icact.org/papersubmission/paper_update_proc.asp HTTP/1.1 Host: icact.org Proxy-Connection: keep-alive Content-Length: 16749 Cache-Control: max-age=0 Origin: http://icact.org Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryzRAAbsnJ8TyEBu7i Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 Referer: http://icact.org/papersubmission/paper_update.asp Accept-Language: ko-KR;q=0.8,en-US;q=0.6,en;q=0.4 Cookie: ASPSESSIONIDAQBBBTQT=CCNNEPNACCPHCHOJDDAKAPOD</pre>		

**Header Part**

**Session(Cookie)**

**Body Part**

```
-----WebKitFormBoundaryzRAAbsnJ8TyEBu7i
Content-Disposition: form-data; name="pno"
20170442
-----WebKitFormBoundaryzRAAbsnJ8TyEBu7i
Content-Disposition: form-data; name="ptitle"
Experimental Validation of Multipoint Joint Processing of Range Measurements via Software-Defined Radio Testbed
-----WebKitFormBoundaryzRAAbsnJ8TyEBu7i
Content-Disposition: form-data; name="keyword"
Analytical model, Distance measurement, Radar signal processing, Radio navigation, Software radio
-----WebKitFormBoundaryzRAAbsnJ8TyEBu7i
Content-Disposition: form-data; name="field"
```







# Cyber Space Protocol – HTTP Response Message Format

```

1. HTTP/1.1 OK 200 // http version, Response Status Code
2. Server: NCSA/1.4.2 // Web Sever version
3. Content-type: text/html // MIME Type (Multipurpose Internet Message Extensions)
4. Content-length: 107 // HTTP Message Body Size
    
```

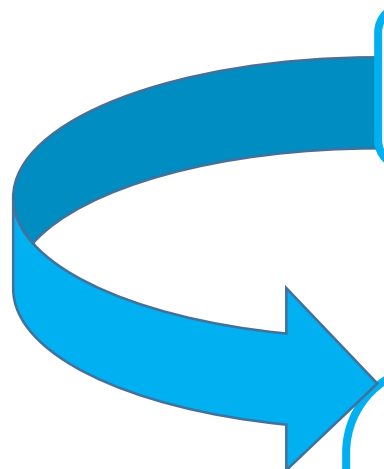
**Header Part**

One Empty Space Line as Separator

```

5. <html>
<head></head> // Requested HTML Webpage
  <Title>http protocol</Title>
  <body>
    The understanding of http protocol
  </body>
</html>
    
```

**Body Part**







## Response Message Scan



Request | Response | Trap

**HTTP/1.1 200 OK** ← HTTP Response Status Code

Date: Tue, 14 Feb 2017 08:28:32 GMT  
Server: Microsoft-IIS/6.0  
X-Powered-By: ASP.NET

**Content-Length: 198081**  
**Content-Type: text/html**  
Cache-control: private

```
<!--2016-10-29-toma-Full paper default-->
<!-- 2012-05-20- edited by toma, provide the Journal-->
<!-- 2010-10-16- edited by toma, provide the uploaded paper view-->

<script type="text/jscript" language="javascript" src="/include/script.js"></script>
<!--toma-->

<html>
<head>
<meta http-equiv=Content-Type content="text/html;charset=euc-kr">
<meta http-equiv=Cache-Control content=No-Cache>
<meta http-equiv=Pragma content=No-Cache>
<title>www.icact.org</title>
<link rel="stylesheet" href="/css/icact.css">
<script language="javascript" src="/include/common.js"></script>
</head>
```

Raw View |  Trap request |  Trap response | Continue | D

## Form based Webpage

mission/paper\_update.asp

### ➤ Paper Information

\* Title of Paper

\* Keyword

\* Topics

\* Upload File  No file chosen PDF file only!

20170442 Paper.pdf <--- Please confirm your latest upload file here!

Do you want to upload your file?  Yes  No

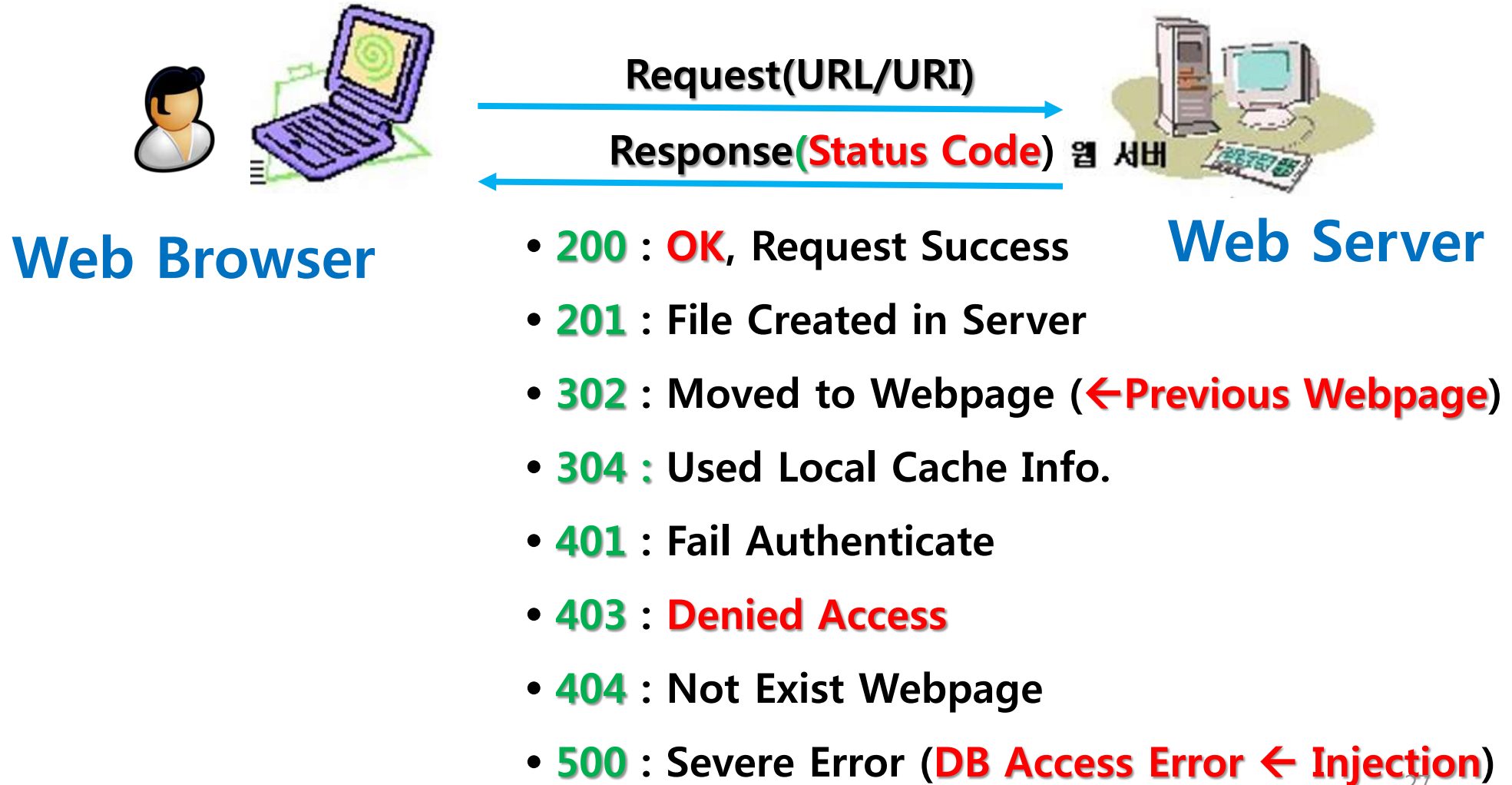
Abstract(1 page)  Full Paper(Min,3 pages)

\* Number of Pages

\* E-mail(One address only)



# Cyber Space Protocol – HTTP Response Status Code



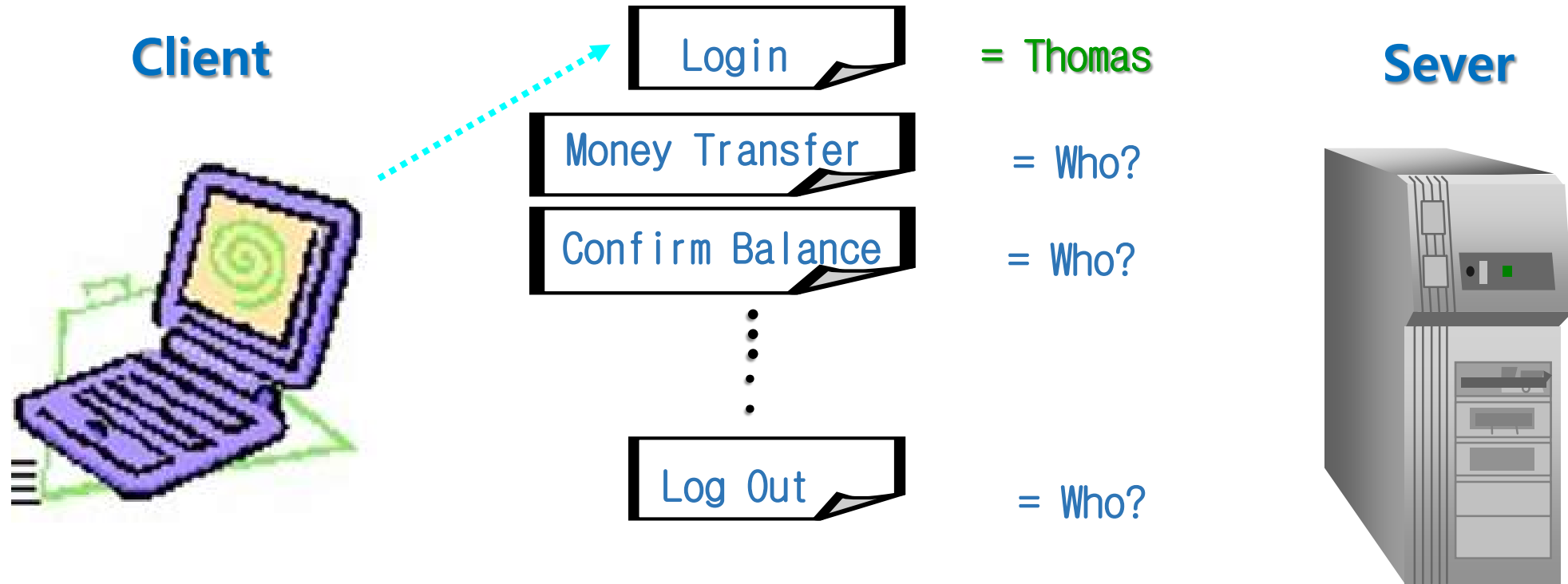




# Cyber Space Web Programing Method – Stateless vs State Oriented

Cyber Space has Huge Users – **Challenge & Chance**

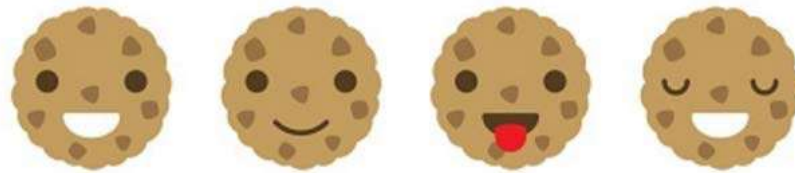
**Pros & Cons** : Web Server Cost Performance, but User Authentication needed



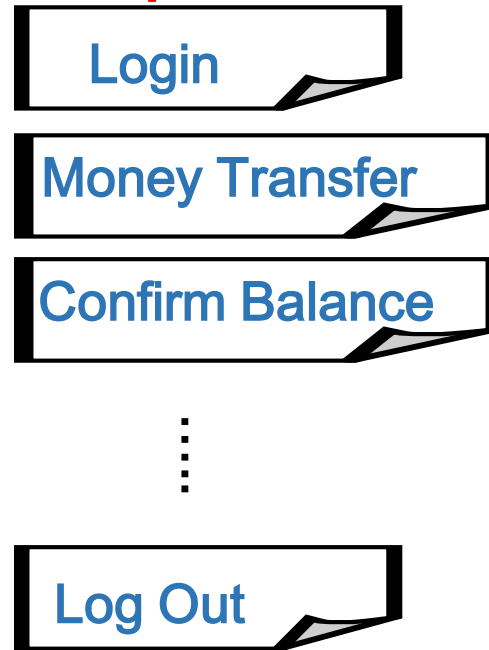
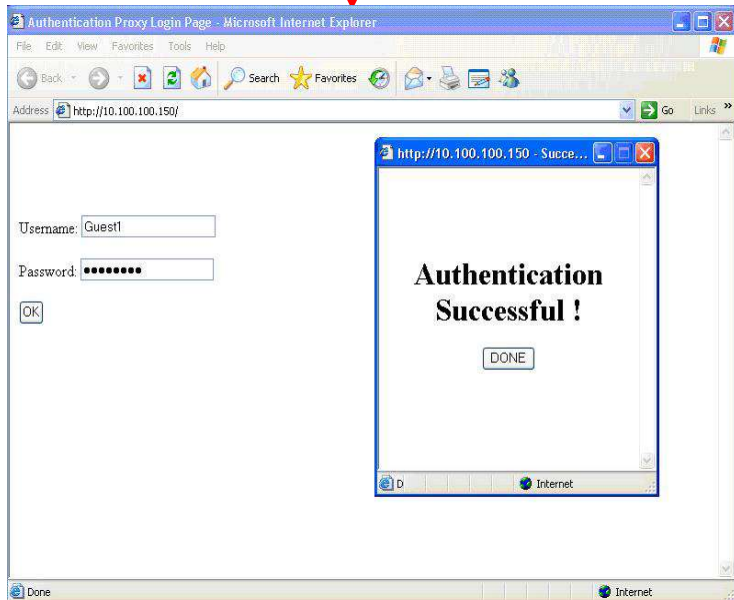
Banking Service Work Flow



## Stateless Web Programming : Cookie

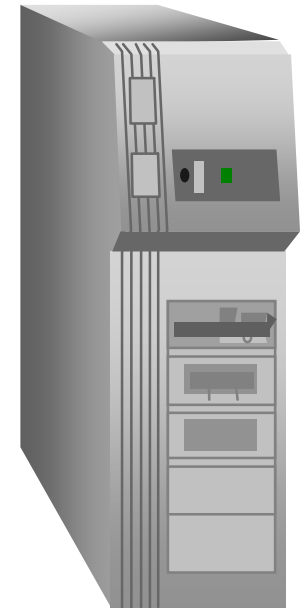


Client Keeps Cookie

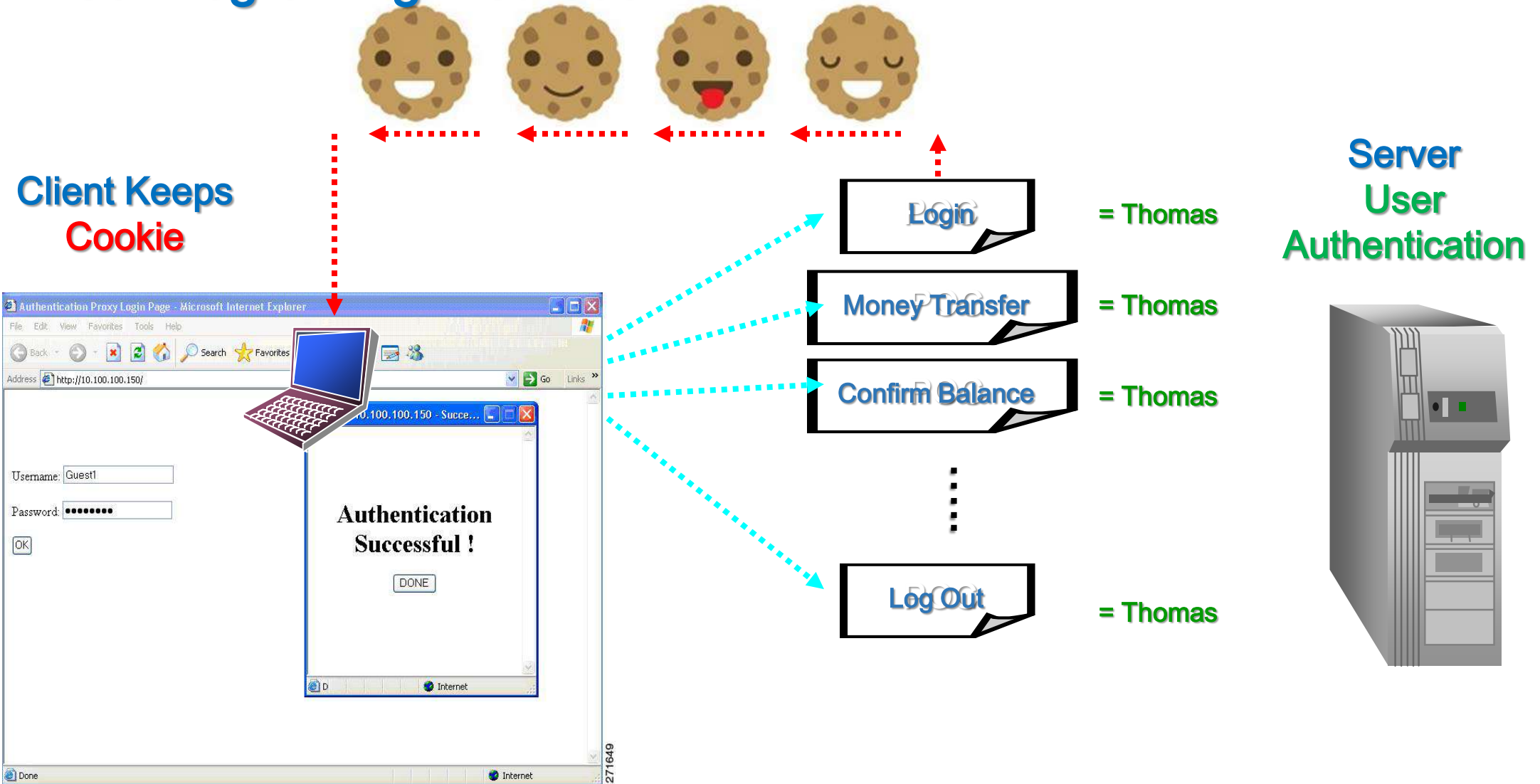


= Thomas  
= Thomas  
= Thomas  
= Thomas

Server  
User  
Authenticate

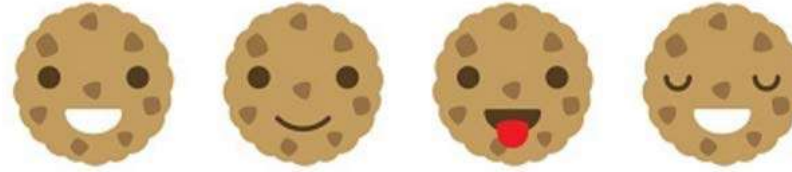


## Stateless Web Programming Methods : **Cookie**





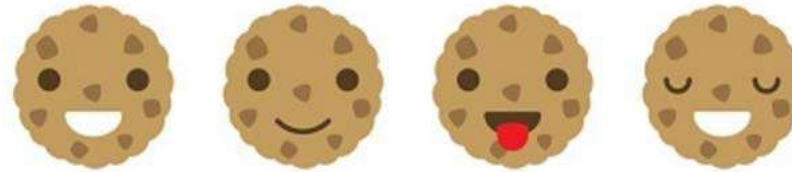
# Stateless Web Programming Methods : **Cookie**



Criteria	Persistence Cookie	Session Cookie
Storage	Disk File	Browser Memory
Life Time	Time-Out Value, Delete by User	Browser End
When Initial Website Connection	Send Cookie	No Send Cookie
Usage	Reconnect Website	Access Webpages



## Stateless Web Programming Methods : **Session Cookie Names**



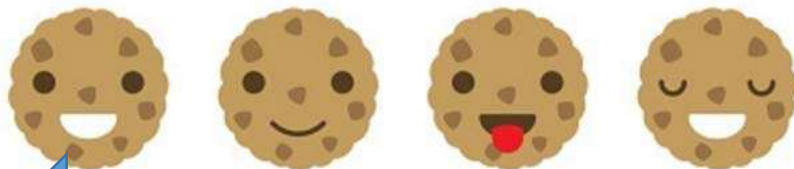
Hidden Parameter	Cookie	Session
Name, Password, Data	+UA	++Session ID
No Expire Time	Time-Out	Browser End
Very Simple	Secure	Very Secure
Store in Client	Store in Client	Critical Date in Server





# Stateless Web Programming Methods : **Cookie**

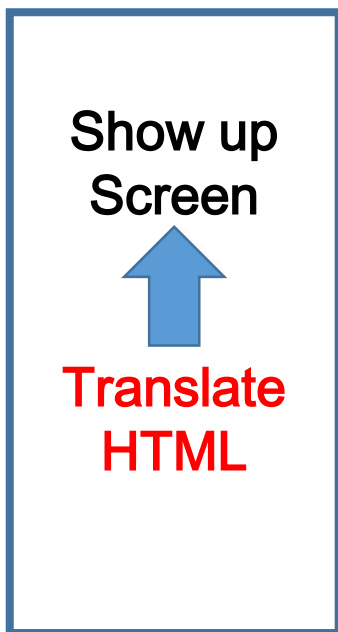
1. Initial request Webpage
4. Store Cookie
5. Request Webpage + Cookie



2. Create Cookie
3. Send Cookie
6. User Authenticate



**Client**



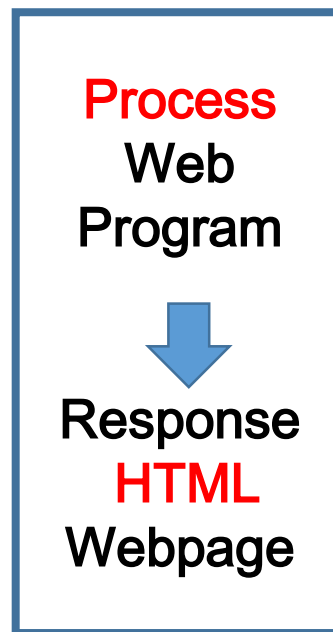
Connect, **Session Start**

Request Webpage (**URL/URI**)

Response (**HTML File**)

Disconnect, **Session End**

**Server**



# Cookie Programming Methods : Hidden Parameter from Server

Report Tools Help

Request	Response	Trap
HTTP/1.1	200 OK	
Date: Sun, 12 Feb 2017 06:03:15 GMT Server: Microsoft-IIS/6.0 X-Powered-By: ASP.NET Content-Length: 532 Content-Type: text/html Cache-control: private		
<pre> &lt;form name="frm" method="post"&gt;   &lt;input type="hidden" name="eMail" value="tomayoon@ieee.org"&gt;   &lt;input type="hidden" name="pwd" value="1111"&gt; &lt;/form&gt;  &lt;script language="javascript"&gt; &lt;!--     alert("tomayoon@ieee.org Authentication Successful! Go to the Annual Scheduler !");     frm.action = "schedule.asp";     frm.submit(); --&gt; &lt;/script&gt;           </pre>		
Raw View	<input type="checkbox"/> Trap request	<input checked="" type="checkbox"/> Trap response
		Continue Drop
n.altools.com/albnInfo?no=1500&bnver=16.4.28.0	406 Not Acceptable	349ms
pdateadd.altools.com/default.ashx?t=3&ios=6,2,2,1,9&p=ALC...	406 Not Acceptable	351ms
/asp/schedule_login.asp	200 OK	2065ms





## Stateless Web Programming Methods : Cookie + Session ID

Untitled Session - Paros

Report Tools Help

Request	Response	Trap
POST http://icact.org/asp/schedule_login_proc.asp HTTP/1.1		
Host: icact.org		
Proxy-Connection: keep-alive		
Content-Length: 34		
Cache-Control: max-age=0		
Origin: http://icact.org		
Upgrade-Insecure-Requests: 1		
User-Agent: Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36		
Content-Type: application/x-www-form-urlencoded		
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8		
Referer: http://icact.org/asp/schedule_login.asp		
Accept-Language: ko-KR;q=0.8,en-US;q=0.6,en;q=0.4		
Cookie: ASPSESSIONIDAQCCBTRS=NOOJLFHCDDOGA0BMCIGIMGAE; ASPSESSIONIDASCBDTQS=EFDNIDEDEDAOFNPEBGHMAMJJ		
eMail=tomayoon%40ieee.org&pwd=1111		

Raw View  Trap request  Trap response

URL	Status	Time
on.altools.com/albnInfo?no=1500&bnver=16.4.28.0	406 Not Acceptable	349ms
updateadd.altools.com/default.ashx?t=3&ios=6,2,2,1,9&p=ALC...	406 Not Acceptable	351ms
/asp/schedule_login.asp	200 OK	2065ms

www.icact.org

icact.org/asp/schedule\_login.asp

Feb 19 - 22, 2017 PHOENIX PARK, PYEONGCHANG, KOREA

### ICACT2017, 19th International Conference on Advanced Communications Technology

Technically Co-sponsored by **IEEE** **IEEE ComSoc**

Home Register

New 319 visitors  
Today: 460 Yesterday: 1038  
Total: 5027161

2017-02-12, Week 7

#### Scheduler Entrance

Type your eMail & Passwd

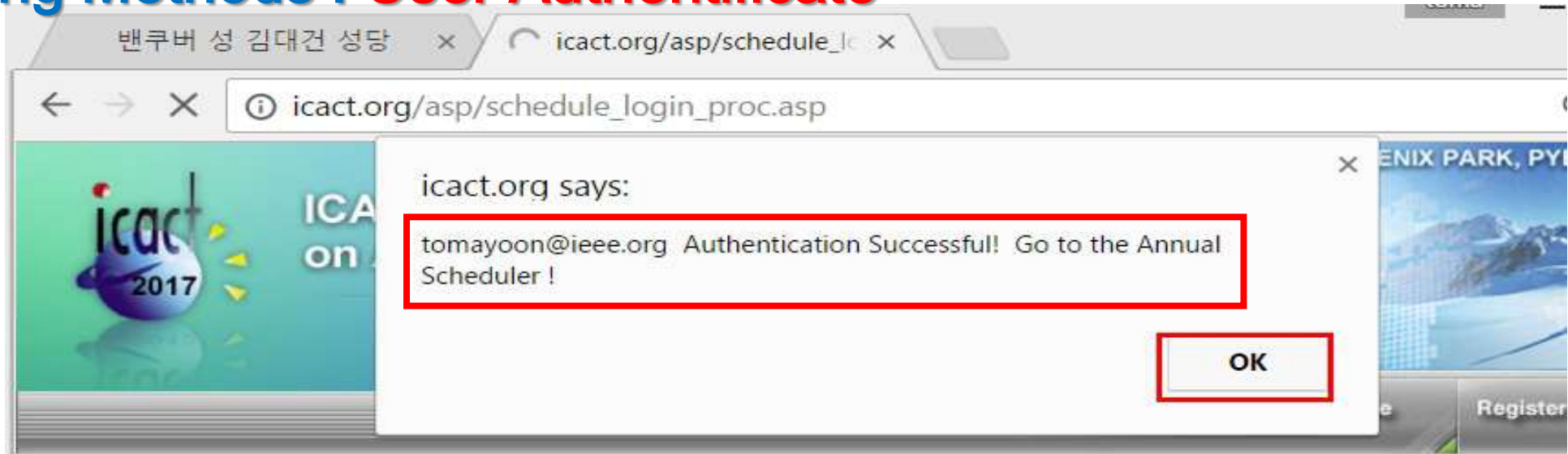
eMail	tomayoon@ieee.org
Password	1111

[Forget your Password?](#)

- Welcome Message
- Statistics & History
- ICACT Committee
- ICACT-TACT Journal
- Paper Archives
- Call For Paper
- Author page**
  - Author Page**
    - Paper Procedure
    - Journal Procedure
    - Presentation



# Cookie Programming Methods : User Authenticate



Now 322 visitors  
Today: 476 Yesterday: 1038  
Total: 5027198

2017-02-12, Week 7

## Scheduler Entrance

Welcome Message

Statistics & History

ICACT Committee

ICACT- TACT Journal

Paper Archives

Call For Paper

Type your eMail & Passwd

eMail	<input type="text" value="tomayoon@ieee.org"/>
Password	<input type="text" value="1111"/>

submit

[Forget your Password?](#)





## Web Service

▶ Giri ( tomayoon@ieee.org )

[Home](#)

[Logout](#)

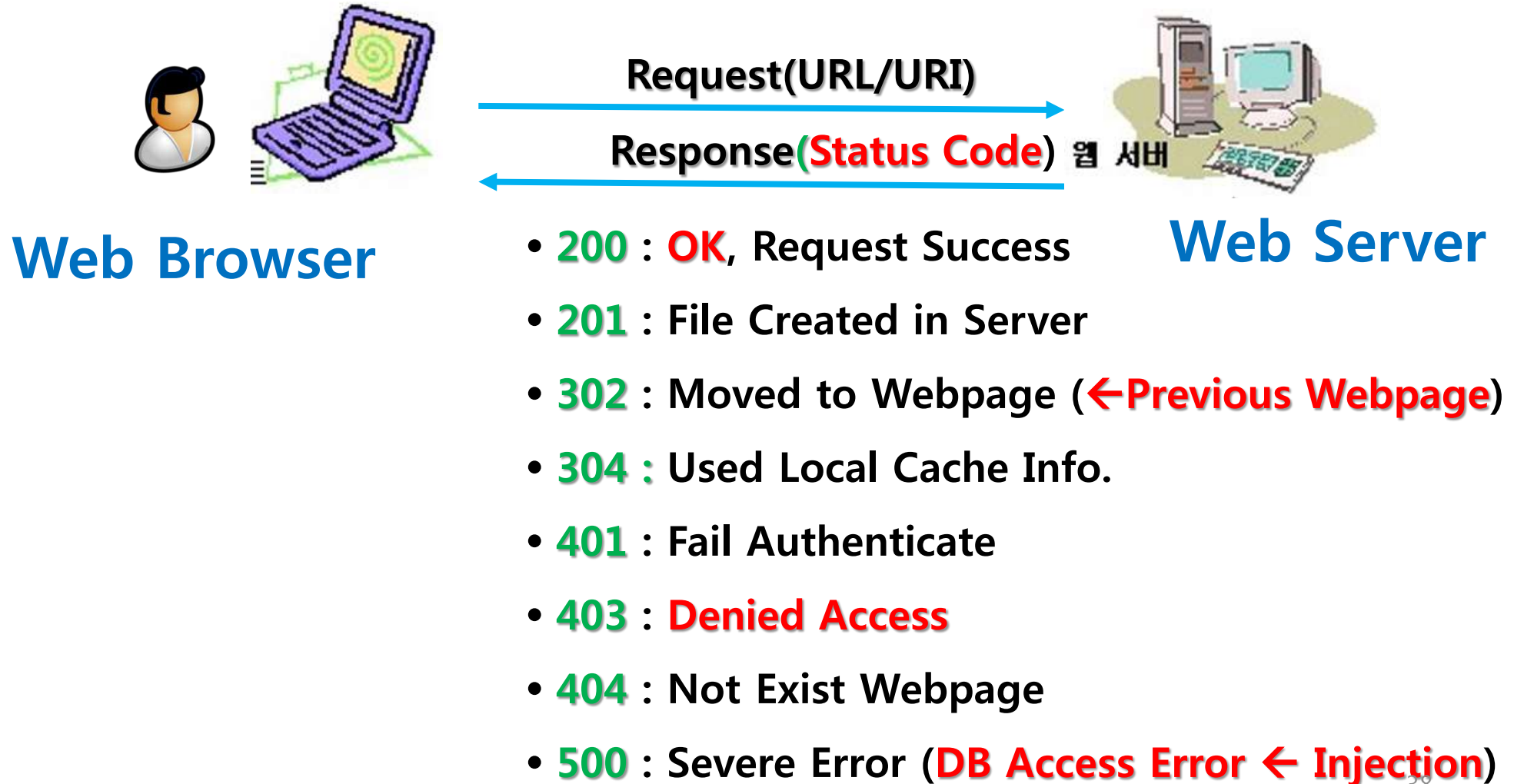
### Annual Schedule

ID\_no(TCSnn, HOMnn, ORGnn, TPCnn, LOCnn) D-day(MM-DD)

CK	ID_no	D-day	Task	InformTo	Owner(eMail)
<input type="checkbox"/>	HOM	01-	ICACT2017 Session Overview with Paper	secretariat@icact.org	tomayoon@eee.org
<input type="checkbox"/>	HOM	02-	ICACT2017 Conference Proceedings	secretariat@icact.org	tomayoon@eee.org
<input type="checkbox"/>	HOM	02-	ICACT2017 KwangWon Convention Bureau	secretariat@icact.org	tomayoon@eee.org
<input type="checkbox"/>	LOC	02-	Invite Session Chair	secretariat@icact.org	tomayoon@eee.org
<input type="checkbox"/>	VIP0	02-	ICACT2017 VIP Invite Confirmation	secretariat@icact.org	tomayoon@eee.org
<input type="checkbox"/>	TCS	05-	Confirm Committee Member	secretariat@icact.org	tomayoon@eee.org
<input type="checkbox"/>	TCS	05-	Invite General Chair	secretariat@icact.org	tomayoon@eee.org
<input type="checkbox"/>	TCS	05-	ICACT2017 CFP PDF	secretariat@icact.org	tomayoon@eee.org



# Cyber Space Protocol – HTTP Response Status Code

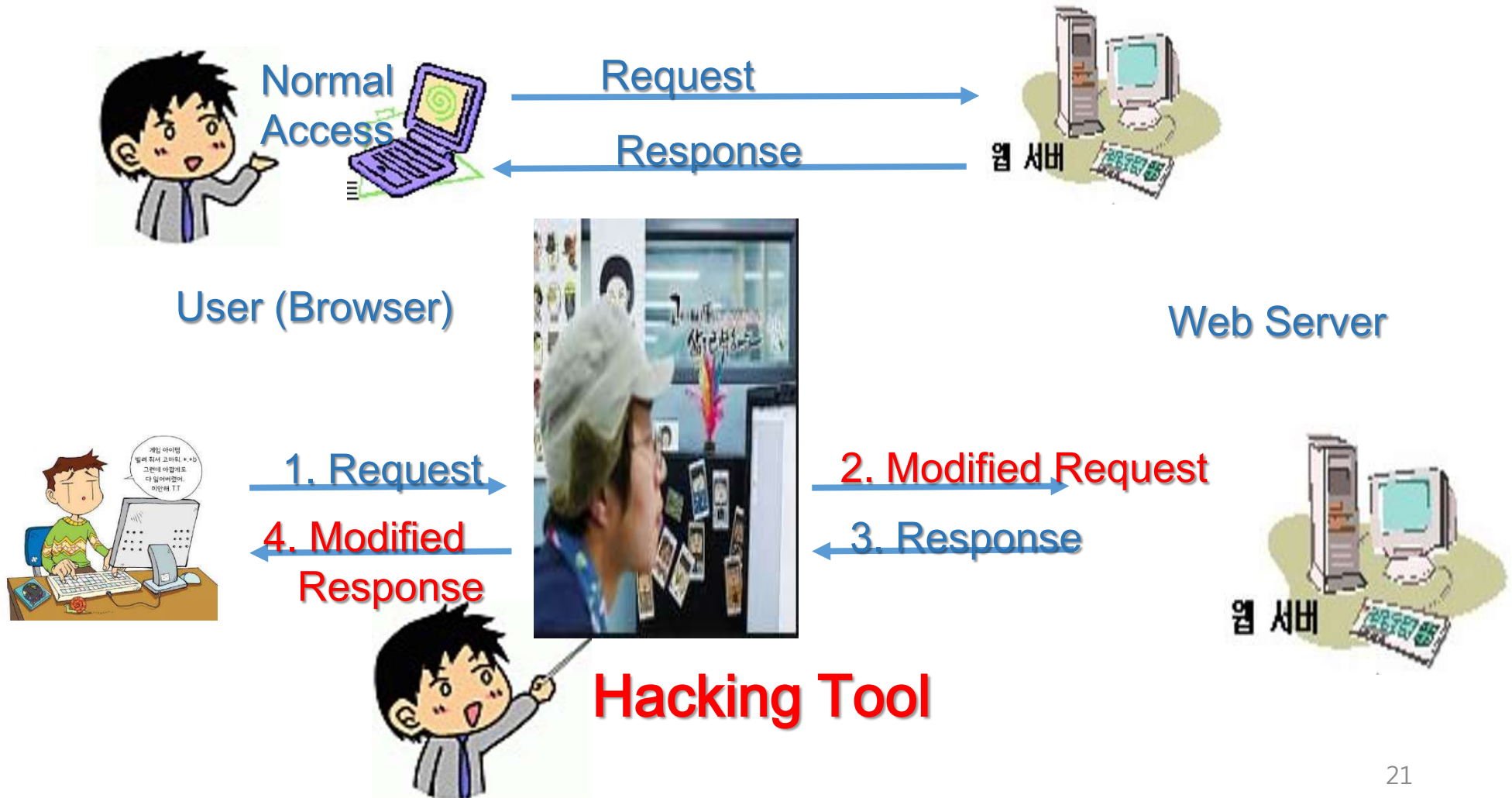


## Web Log Analysis Scan

GET	http://icact.org/index.asp	200 OK	628ms
GET	http://icact.org/manage/index.asp	302 Object moved	635ms
GET	http://icact.org/manage/review/paper_list.asp	404 Not Found	10ms
GET	http://icact.org/manage/review/paper_list.asp	404 Not Found	14ms
GET	http://icact.org/program/papers.asp	200 OK	2832ms
GET	http://icact.org/upload/2016/0004/20160004_biography.pdf	200 OK	125ms
GET	http://icact.org/asp/schedule_login.asp	200 OK	361ms
POST	http://icact.org/asp/schedule_login_proc.asp	200 OK	14ms
POST	http://icact.org/asp/schedule.asp	200 OK	23ms
POST	http://icact.org/asp/Schedule_proc.asp	500 Internal Server Error	18ms
GET	http://icact.org/index.asp	200 OK	607ms
GET	http://icact.org/manage/index.asp	302 Object moved	540ms
GET	http://icact.org/manage/review/paper_list.asp	404 Not Found	9ms



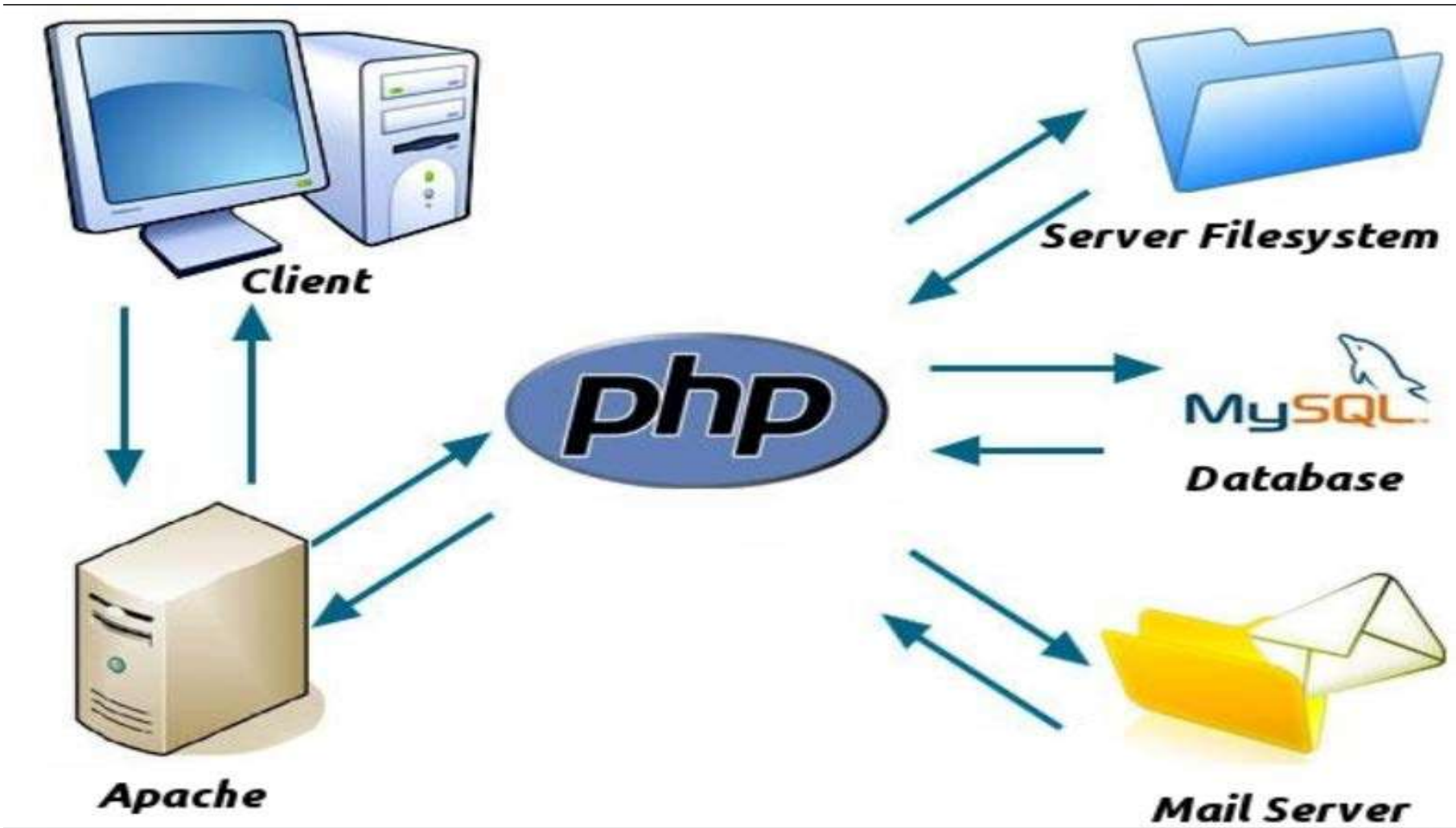
# Hacking Concept - HTTP Intercept







# Where are Hacking Points?!





# Paros – Open Source HTTP Intercept Tool!!



# HTTP Intercept Tool - **Paros!!**

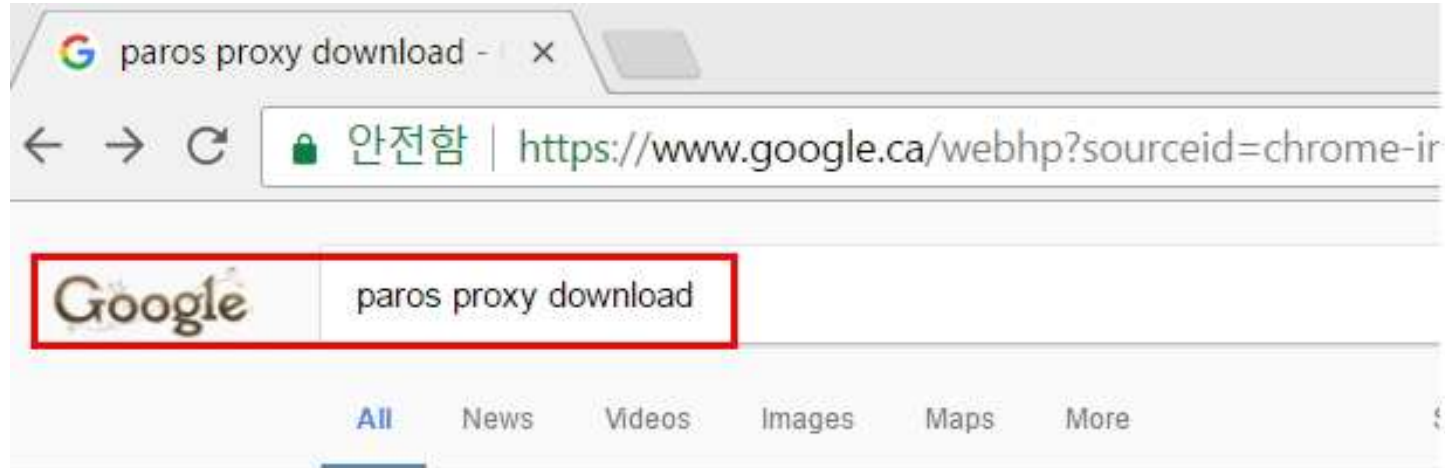
## Paros Client Proxy Capability

- **HTTP Analysis Capability**
- **Web Server Hacking**
- **Vulnerable Point Analysis**





# HTTP Intercept Tool – Paros Installation !!



About 34,200 results (0.61 seconds)

[Paros download | SourceForge.net](https://sourceforge.net/projects/paros/)

<https://sourceforge.net/projects/paros/>

★ ★ ★ ★ ★ Rating: 2.7 - 6 votes

Aug 14, 2013 - Download paros-3.2.13-win.exe. A Java based HTTP/HTTPS proxy for application vulnerability. ... Other features include spiders, client certificate, proxy-chain scanning for XSS and SQL injections etc.

[Paros - Browse /Paros/Version 3.2.13 at SourceForge.net](https://sourceforge.net/projects/paros/files/Paros/Version%203.2.13/)

<https://sourceforge.net/projects/paros/files/Paros/Version%203.2.13/>

A Java based HTTP/HTTPS proxy for assessing web application vulnerability. It supports paros-3.2.13-win.exe (1.7 MB). Home / Paros / Version ...

## HTTP Intercept Tool – Paros Installation !!

Paros download | Source x

← → ↻ 안전함 | <https://sourceforge.net/projects/paros/>

Home / Browse / Security & Utilities / Security / Paros

### Paros

Brought to you by: paros, yukusan

Summary | Files | Reviews | Support | Wiki | Tickets ▾ | Discussion | Code

★ 2.7 Stars (6)  
↓ 698 Downloads (This Week)  
📅 Last Update: 2013-08-14

**Download**  
paros-3.2.13-win.exe

[Browse All Files](#)

Tweet 1 좋아요 5

### Description

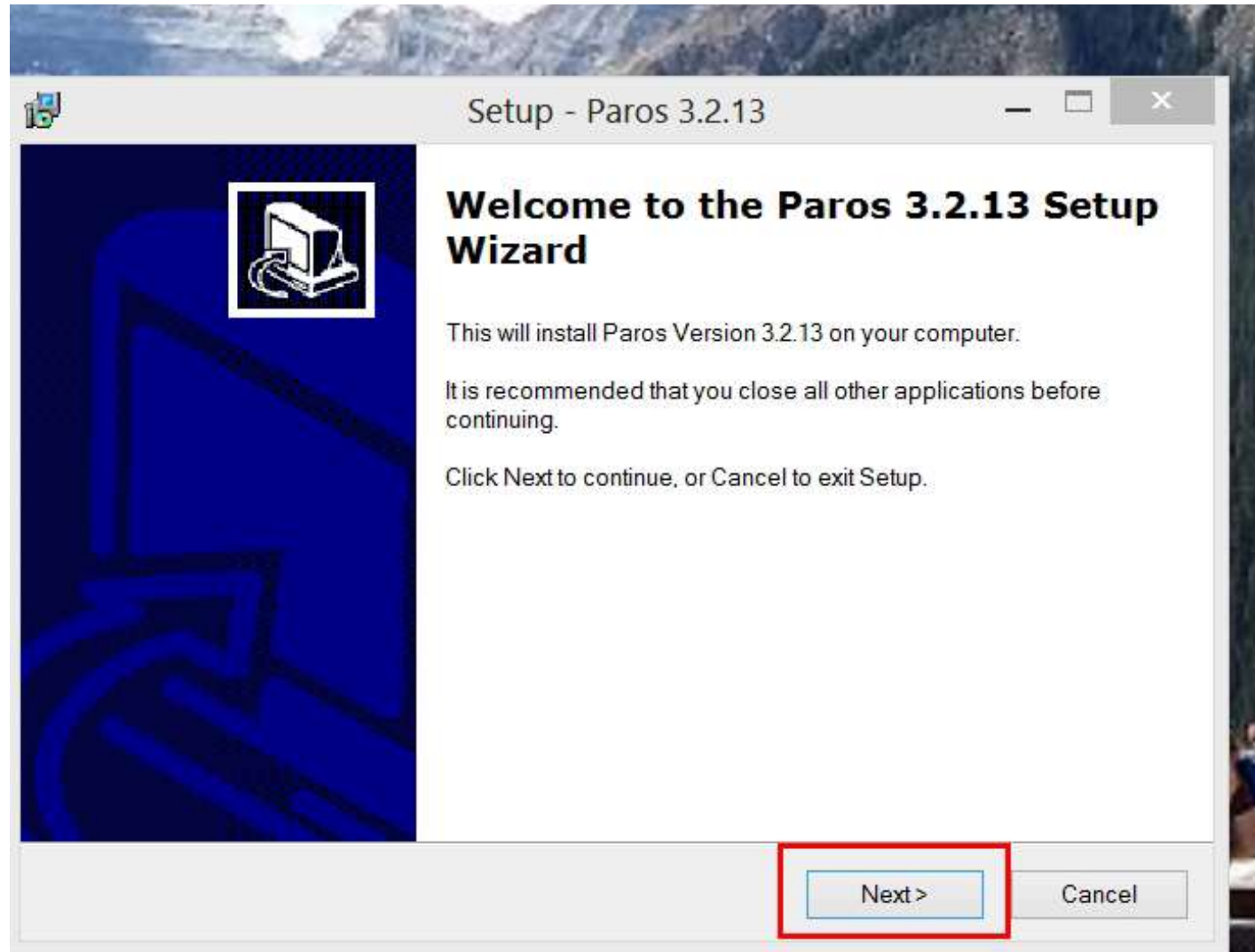
A Java based HTTP/HTTPS proxy for assessing web application vulnerability. It supports editing/viewing HTTP messages on-the-fly. Other features include spiders, client certificate, proxy-chaining, intelligent scanning for XSS and SQL injections etc.

[Paros Web Site](#)

**Categories**  
Security

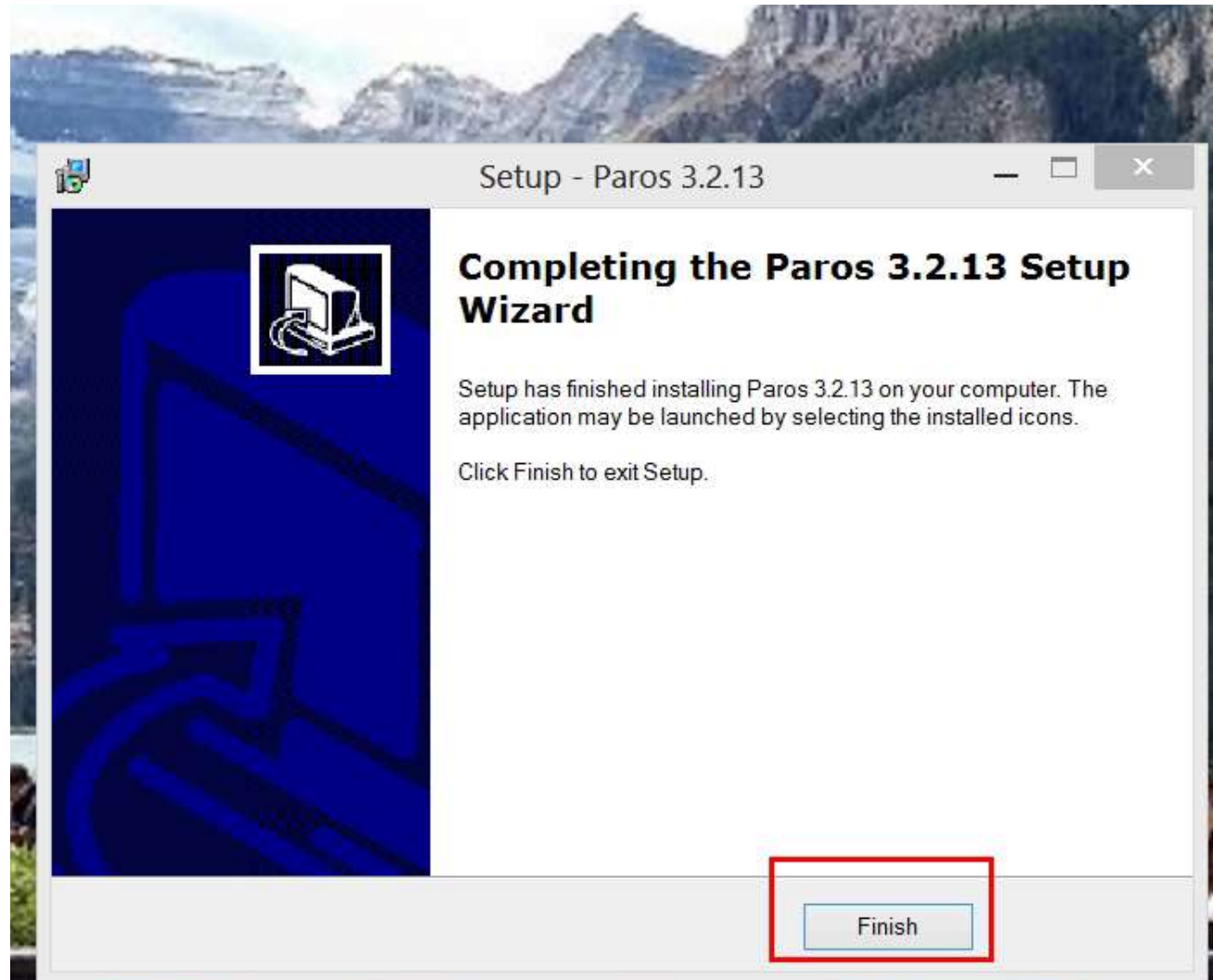
**License**  
Artistic License

# HTTP Intercept Tool – Paros Installation !!

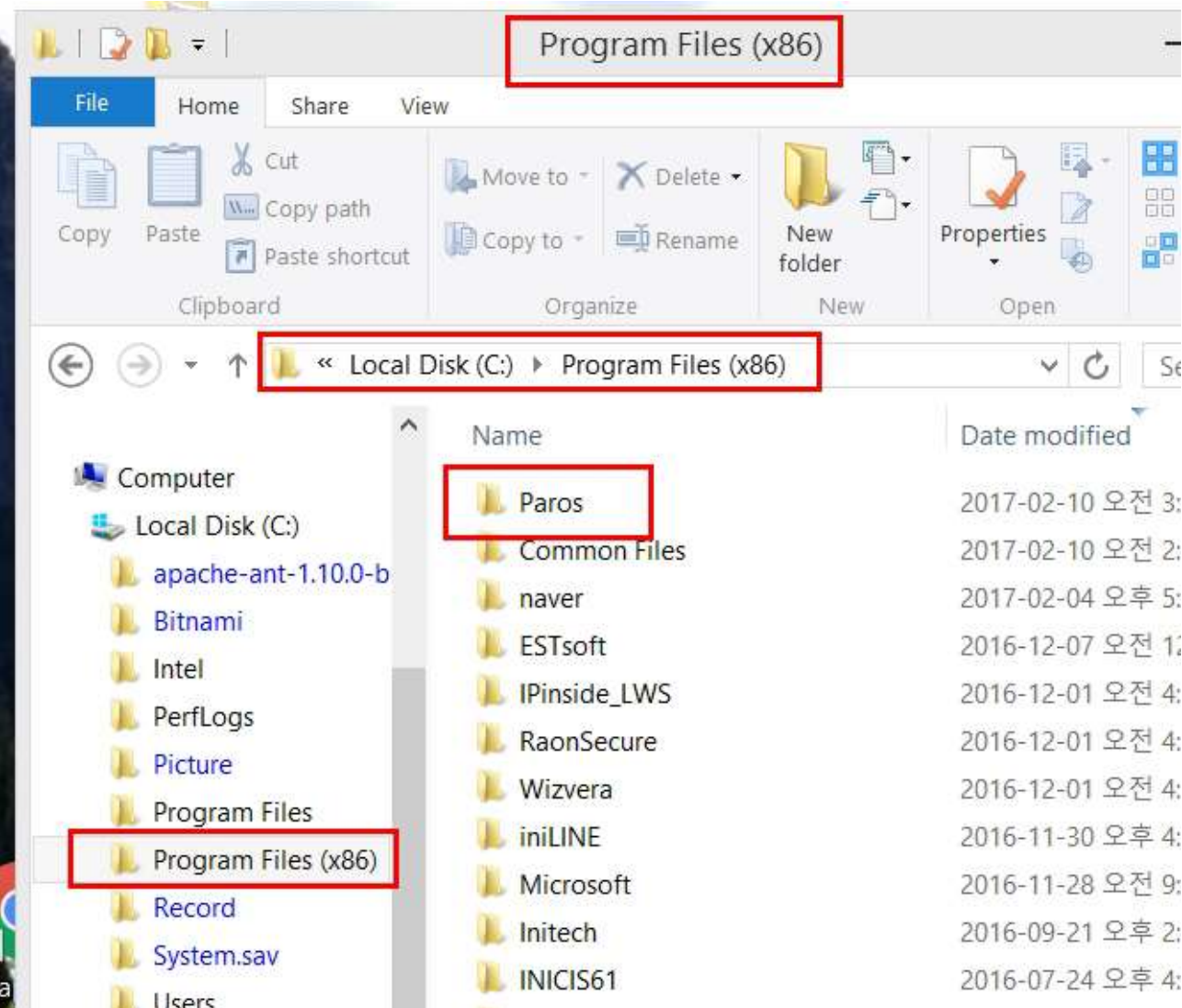




# HTTP Intercept Tool – Paros Installation !!



# Paros Developed for x86 environment only



# Paros Execution

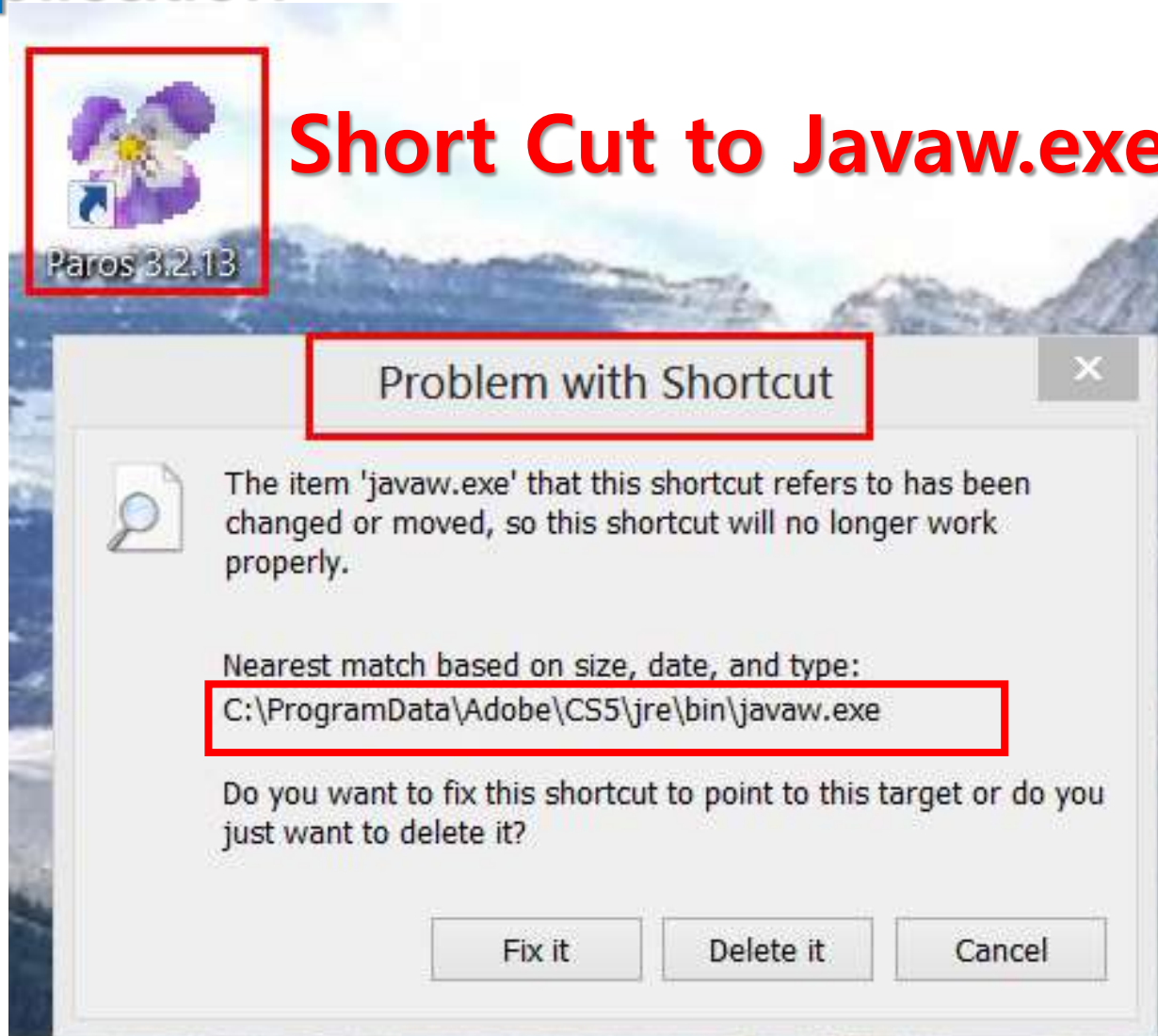




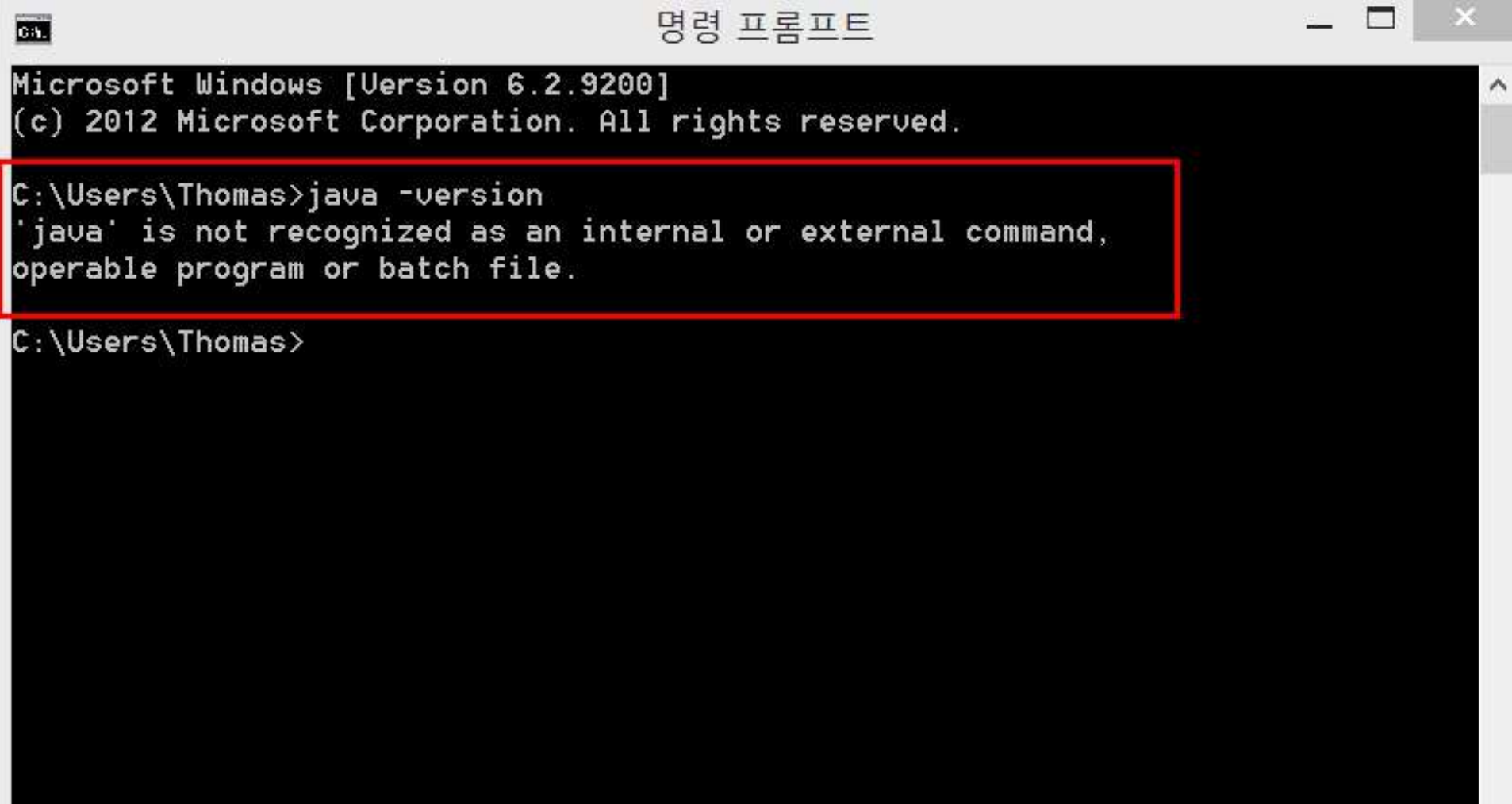
# Paros is Java Application



## Short Cut to Javaw.exe



# Paros needs JDK

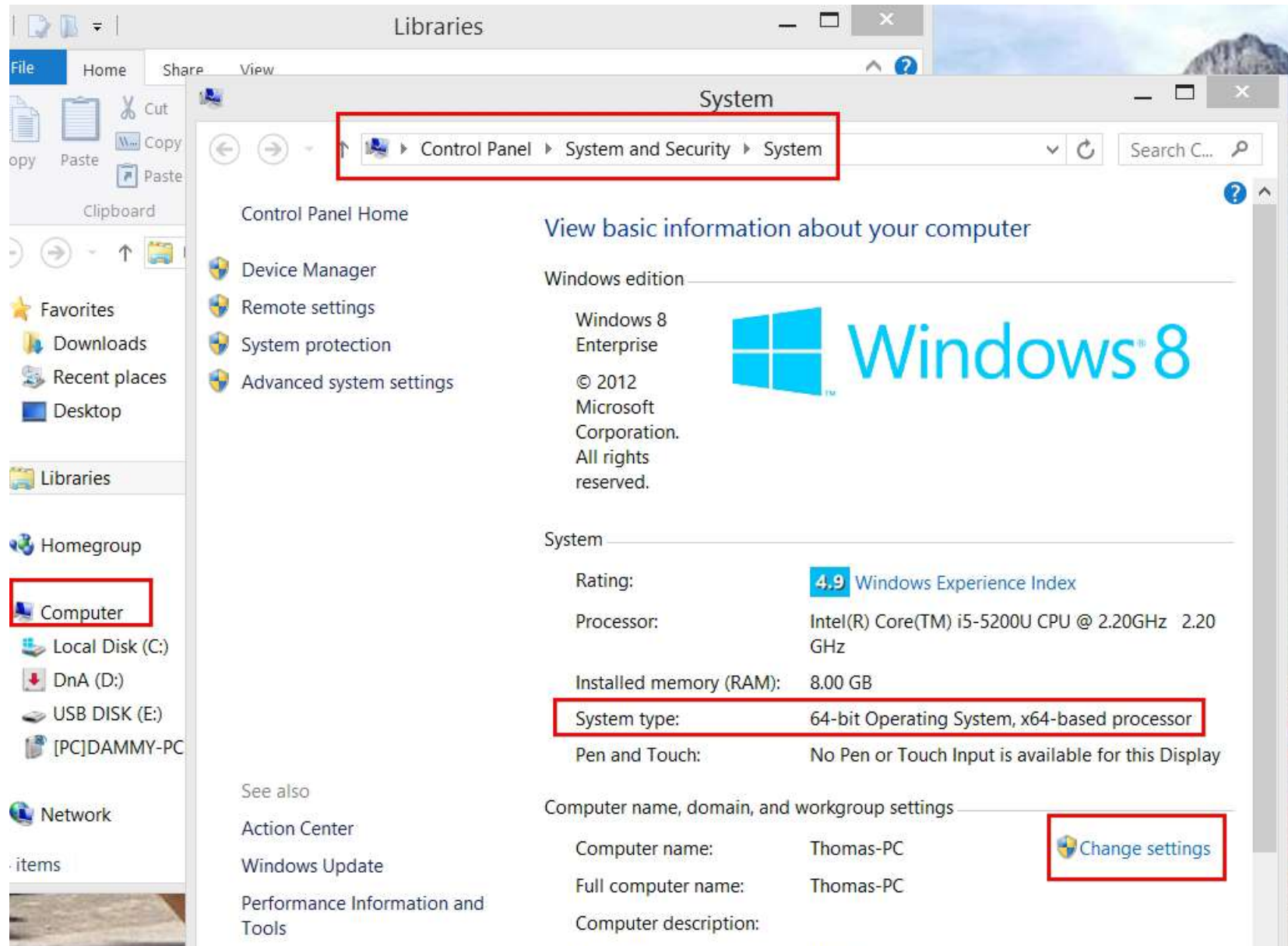


```
명령 프롬프트
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Thomas>java -version
'java' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Thomas>
```

## JDK Installation !!



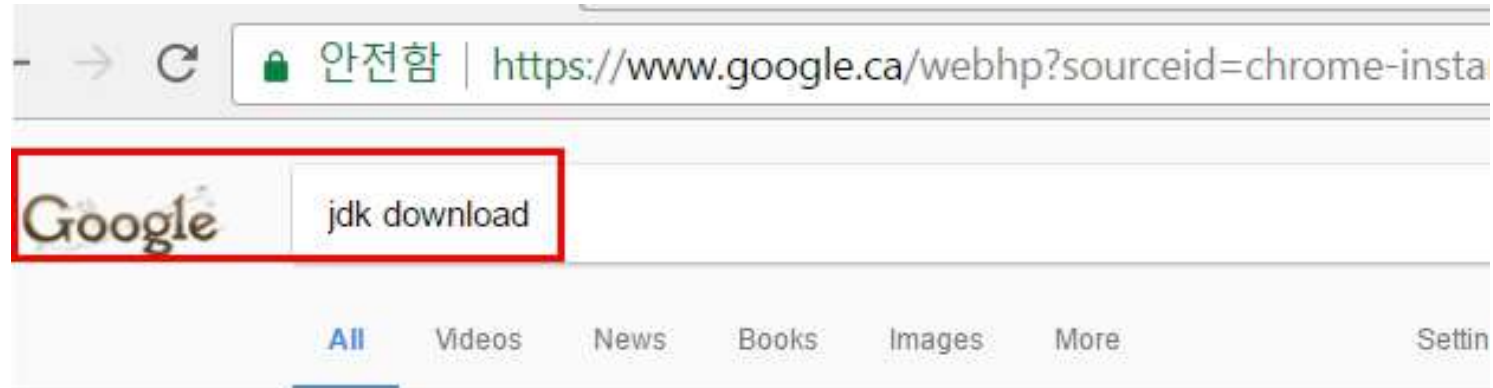
The screenshot shows the Windows 8 System information window. The navigation path in the address bar is **Control Panel > System and Security > System**, which is highlighted with a red box. In the left sidebar, the **Computer** link is also highlighted with a red box. The main content area displays the following system information:

- Windows edition: Windows 8 Enterprise
- © 2012 Microsoft Corporation. All rights reserved.
- System Rating: **4.9** Windows Experience Index
- Processor: Intel(R) Core(TM) i5-5200U CPU @ 2.20GHz 2.20 GHz
- Installed memory (RAM): 8.00 GB
- System type: 64-bit Operating System, x64-based processor** (highlighted with a red box)
- Pen and Touch: No Pen or Touch Input is available for this Display

At the bottom, under "Computer name, domain, and workgroup settings", the computer name is Thomas-PC, and the **Change settings** button is highlighted with a red box.



# JDK Installation !!



About 674,000 results (0.82 seconds)

Java SE - Downloads | Oracle Technology Network | Oracle  
[www.oracle.com/technetwork/java/.../downloads/index-jsp-138363.html](http://www.oracle.com/technetwork/java/.../downloads/index-jsp-138363.html) ▾  
 Java SE downloads including: Java Development Kit (JDK), Server Java Runtime Environment (Server JRE), and Java Runtime Environment (JRE).

**Java SE Development Kit 8**

Java SE Development Kit 8  
 Downloads. Thank you for ...

Java SE Runtime Environmei

Java SE Runtime Environment 8  
 Downloads. Do you want to run ...

Java SE Downloads

NetBeans - Java FX - Java - Java EE -  
 ...

Server JRE (Java SE Runtime

Server JRE (Java SE Runtime ... The  
 Server JRE is a runtime ...














More results from oracle.com »

# JDK Installation – x86

## Java SE Development Kit 8u121

You must accept the Oracle Binary Code License Agreement for Java SE to download this software.

**Accept License Agreement**
     
  Decline License Agreement

Product / File Description	File Size	Download
Linux ARM 32 Hard Float ABI	77.86 MB	 jdk-8u121-linux-arm32-vfp-hflt.tar.gz
Linux ARM 64 Hard Float ABI	74.83 MB	 jdk-8u121-linux-arm64-vfp-hflt.tar.gz
Linux x86	162.41 MB	 jdk-8u121-linux-i586.rpm
Linux x86	177.13 MB	 jdk-8u121-linux-i586.tar.gz
Linux x64	159.96 MB	 jdk-8u121-linux-x64.rpm
Linux x64	174.76 MB	 jdk-8u121-linux-x64.tar.gz
Mac OS X	223.21 MB	 jdk-8u121-macosx-x64.dmg
Solaris SPARC 64-bit	139.64 MB	 jdk-8u121-solaris-sparcv9.tar.Z
Solaris SPARC 64-bit	99.07 MB	 jdk-8u121-solaris-sparcv9.tar.gz
Solaris x64	140.42 MB	 jdk-8u121-solaris-x64.tar.Z
Solaris x64	96.9 MB	 jdk-8u121-solaris-x64 tar.gz
<b>Windows x86</b>	189.36 MB	 jdk-8u121-windows-i586.exe
Windows x64	195.51 MB	 jdk-8u121-windows-x64.exe

## Java SE Development Kit 8u121 Demos and Samples Downloads



# JDK Installation !!

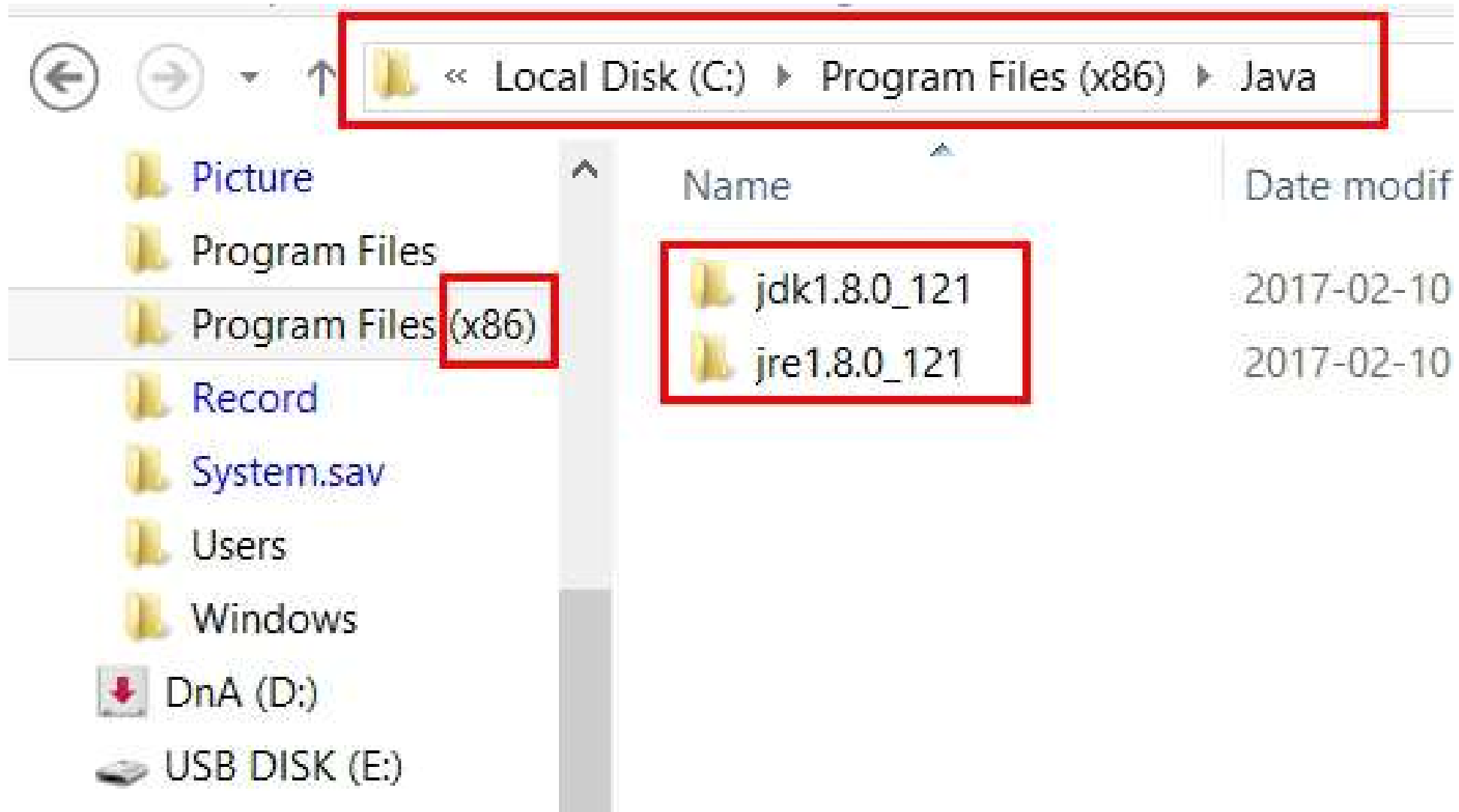




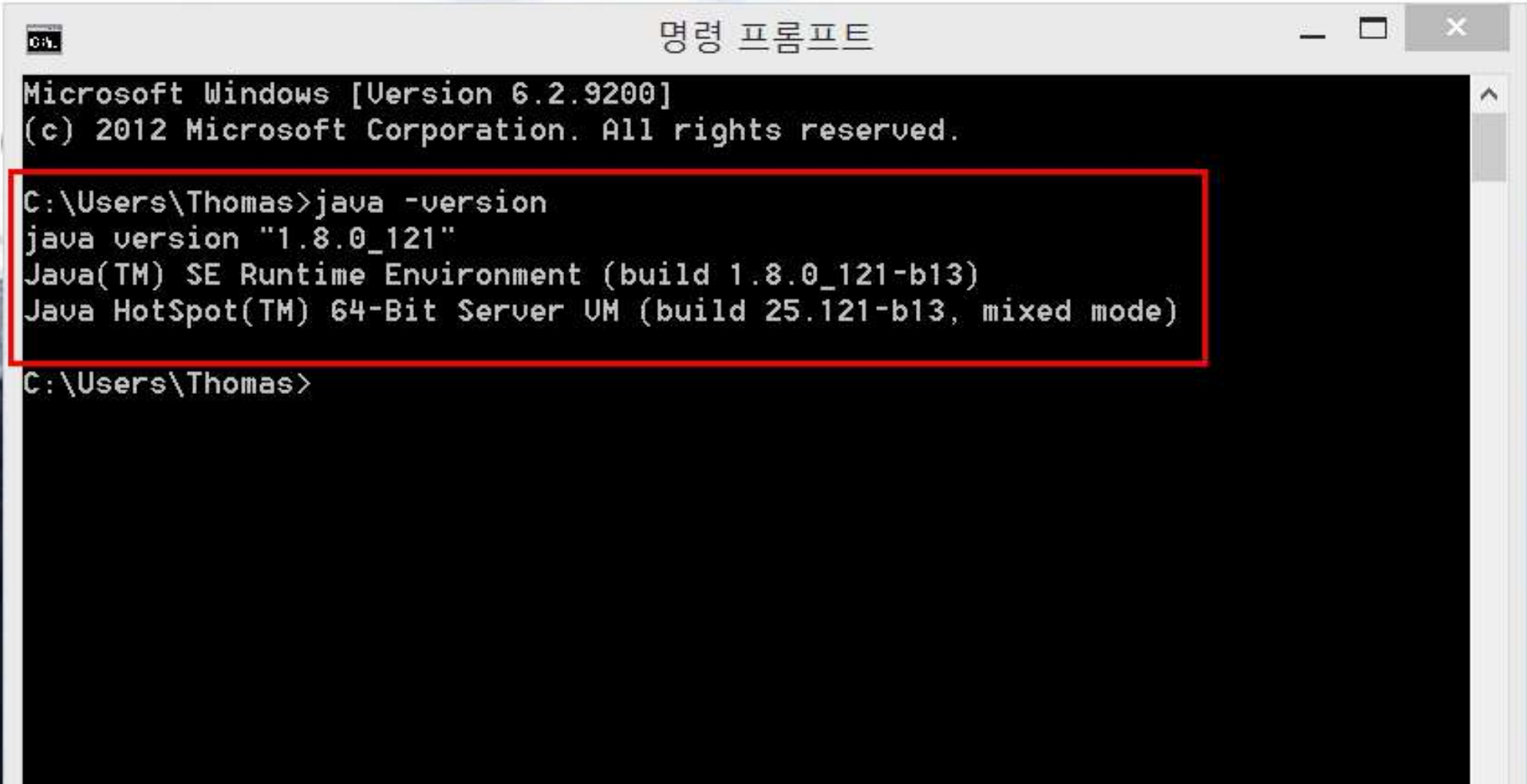
# JDK Installation Completed !!



## JDK Installation x86 - Confirm !!



## JDK Installation - Confirm !!



```
명령 프롬프트
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Thomas>java -version
java version "1.8.0_121"
Java(TM) SE Runtime Environment (build 1.8.0_121-b13)
Java HotSpot(TM) 64-Bit Server VM (build 25.121-b13, mixed mode)

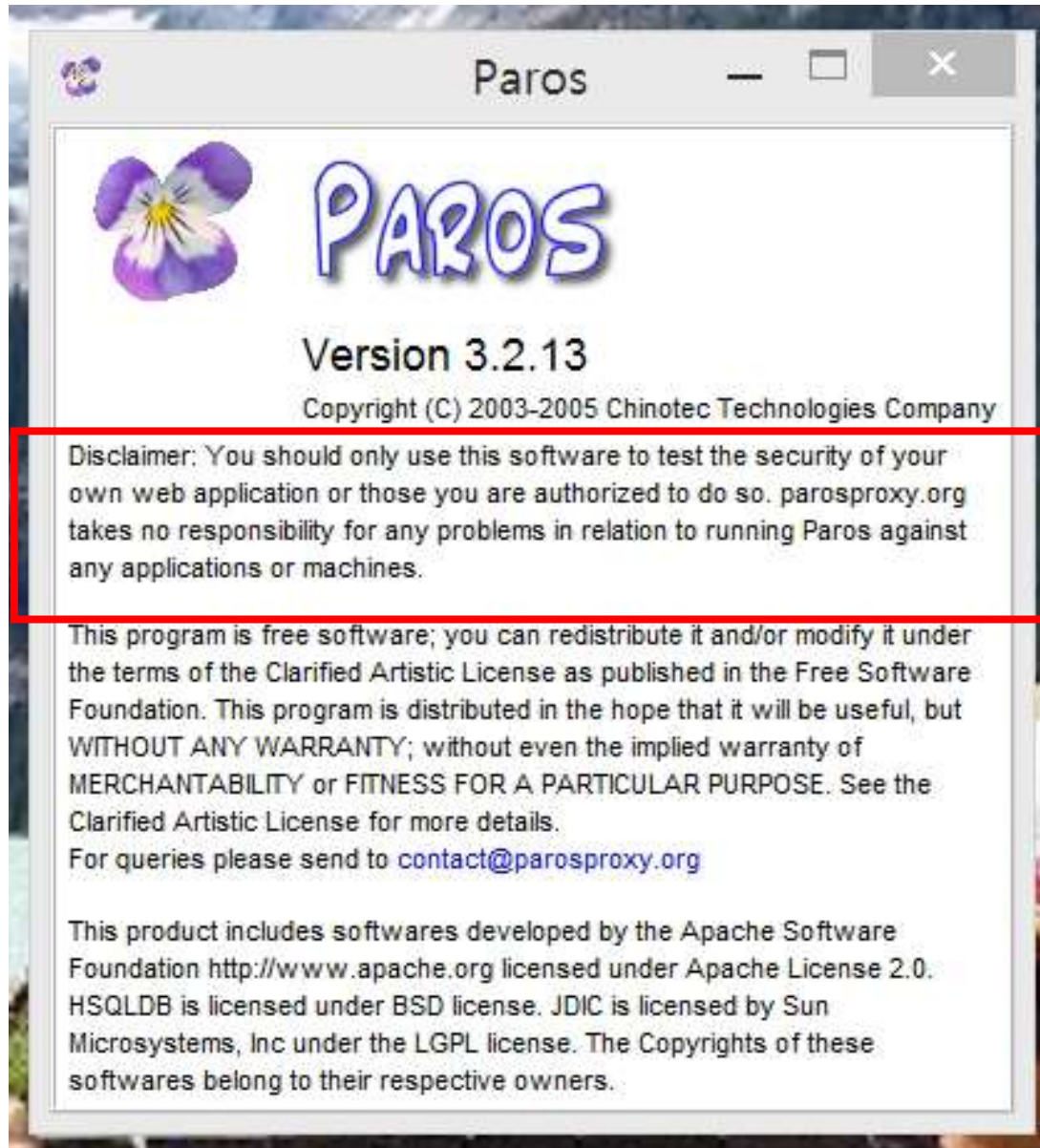
C:\Users\Thomas>
```



## PAROS Execution

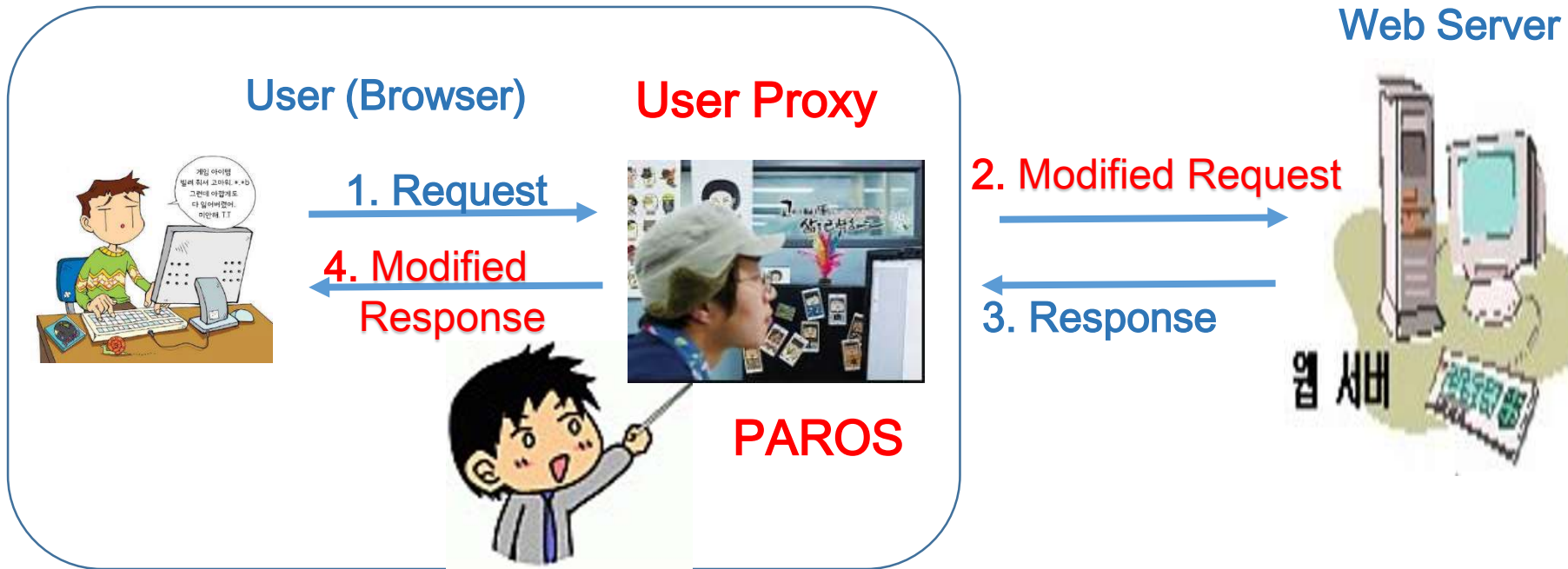
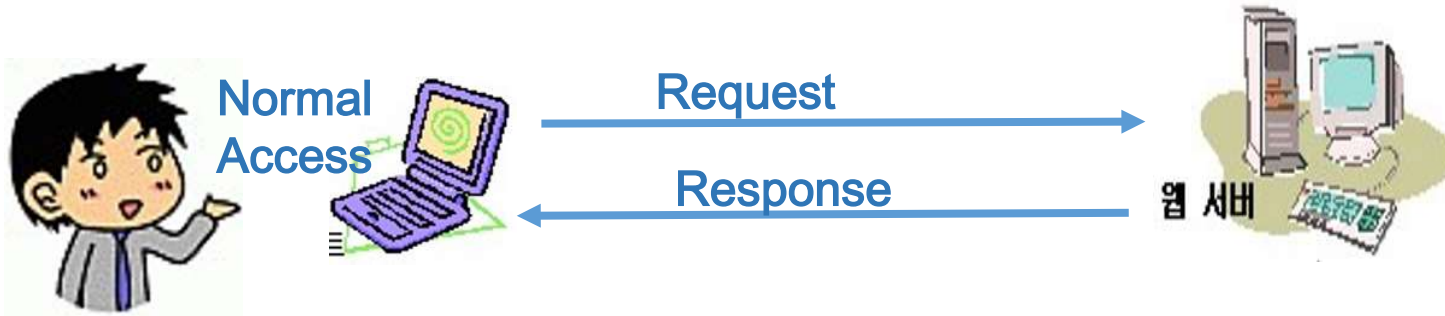


## PAROS Execution





# HTTP Intercept – PAROS Ready to Use!





# Cyber Space Hacking Tool – Paros

## ○ Paros Main Functional Modules

1. **Crawl** : Collect URL Structure, Webpage Information
2. **Scan** : Find Vulnerable Pattern by Collected Information
3. **Report** : Report Vulnerable Points
4. **Proxy** : Provide HTTP Proxy Platform

# Proxy Server Setting IE Browser

The screenshot shows the Internet Options dialog box in Internet Explorer. The 'Connections' tab is selected. The 'LAN settings' button is highlighted with a red box. The 'Dial-up and Virtual Private Network settings' section is also visible, with the 'LAN settings' button highlighted. The 'Local Area Network (LAN) settings' section is also visible, with the 'LAN settings' button highlighted.

Internet Options

General Security Privacy Content **Connections** Programs Advanced

To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

Choose Settings if you need to configure a proxy server for a connection.

Never dial a connection  
 Dial whenever a network connection is not present  
 Always dial my default connection

Current None

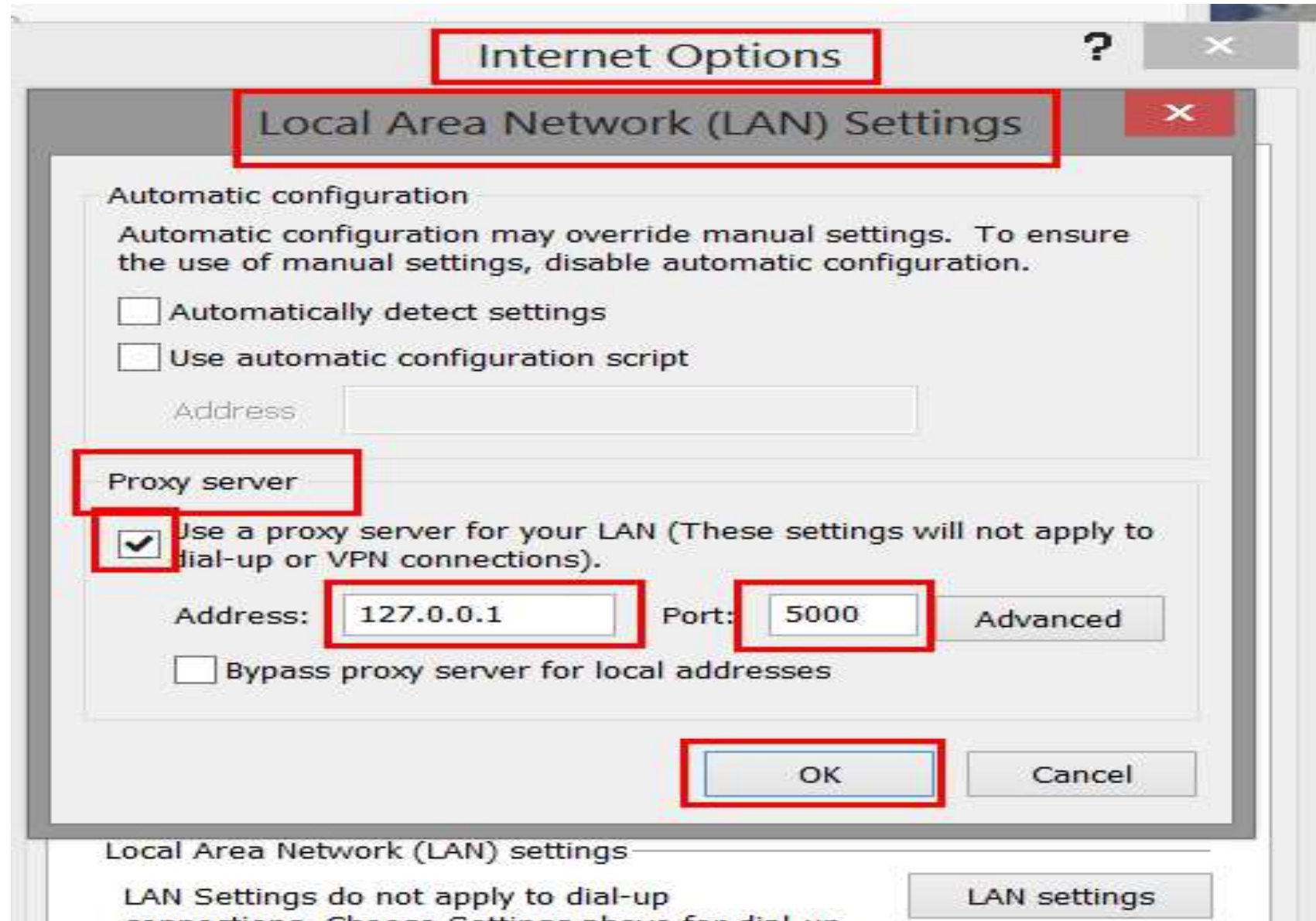
Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

LAN settings

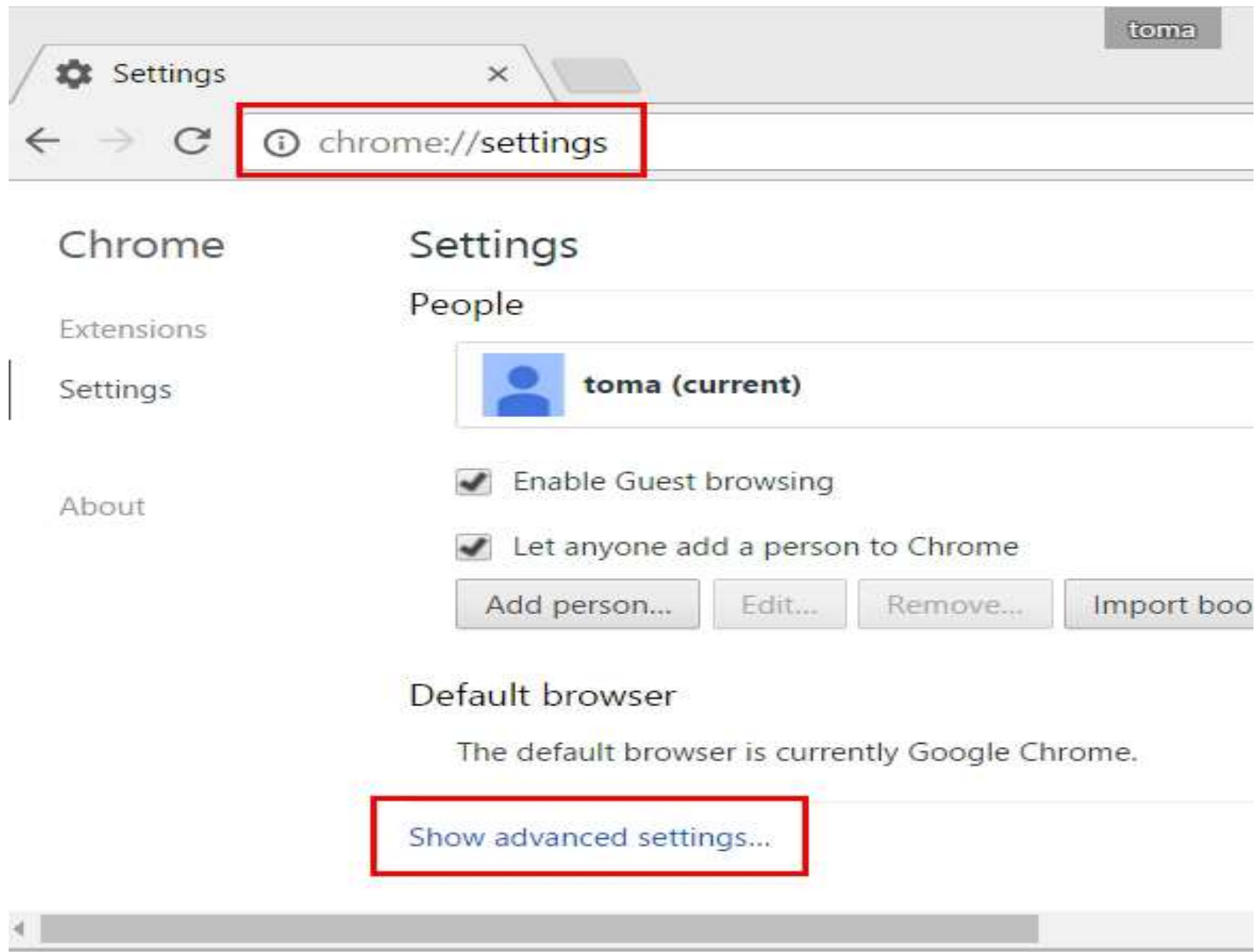
OK Cancel Apply

# Proxy Server Setting IE Browser





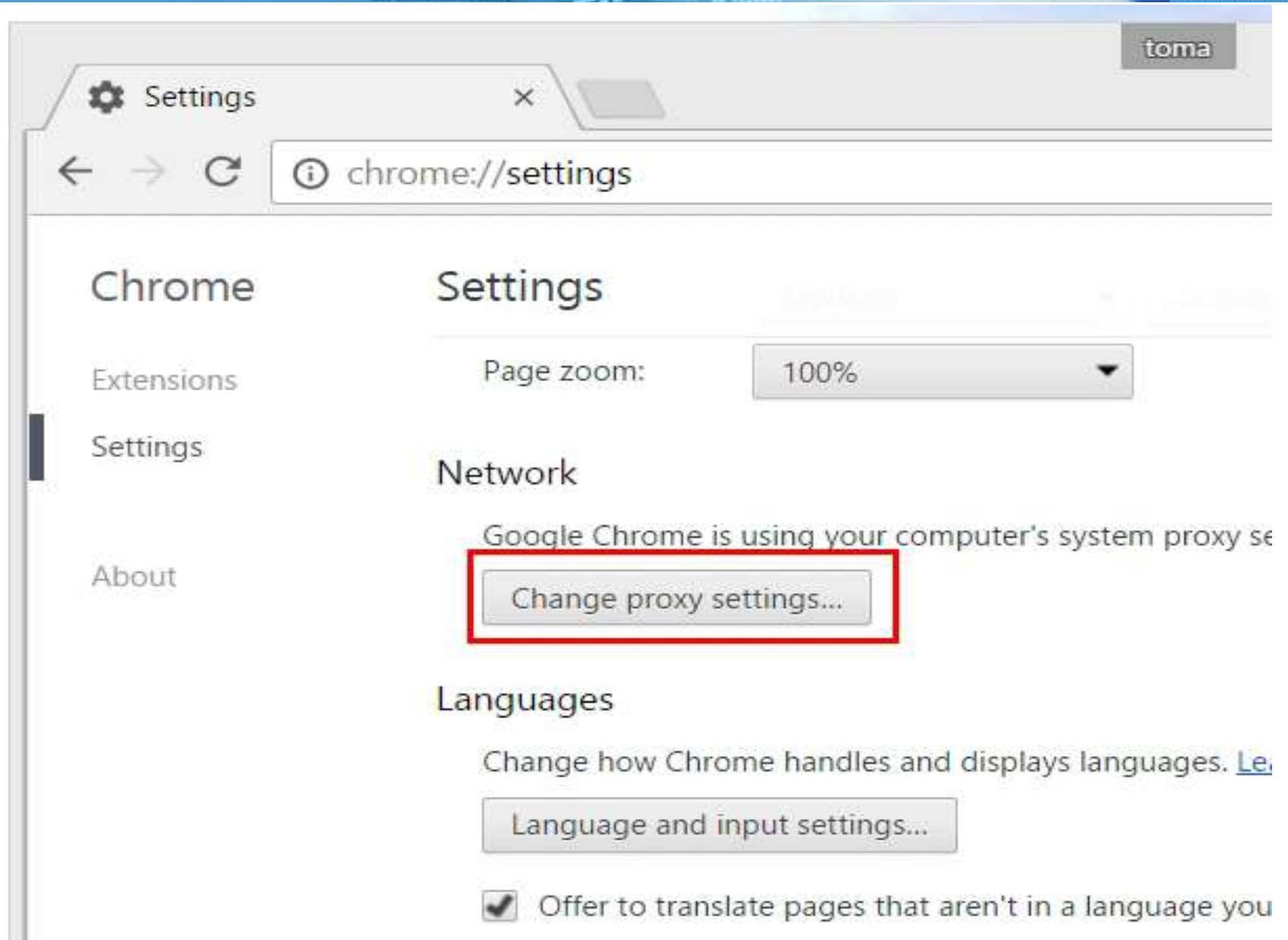
# Proxy Server Setting Chrome Browser



The screenshot shows the Chrome browser interface with the Settings page open. The address bar at the top contains the URL `chrome://settings`, which is highlighted with a red box. The left sidebar shows the navigation menu with 'Settings' selected. The main content area is titled 'Settings' and includes a 'People' section with a user profile for 'toma (current)'. Below this, there are two checked options: 'Enable Guest browsing' and 'Let anyone add a person to Chrome'. At the bottom of the visible settings, there is a 'Default browser' section stating 'The default browser is currently Google Chrome.' A red box highlights the 'Show advanced settings...' link at the bottom of the page.

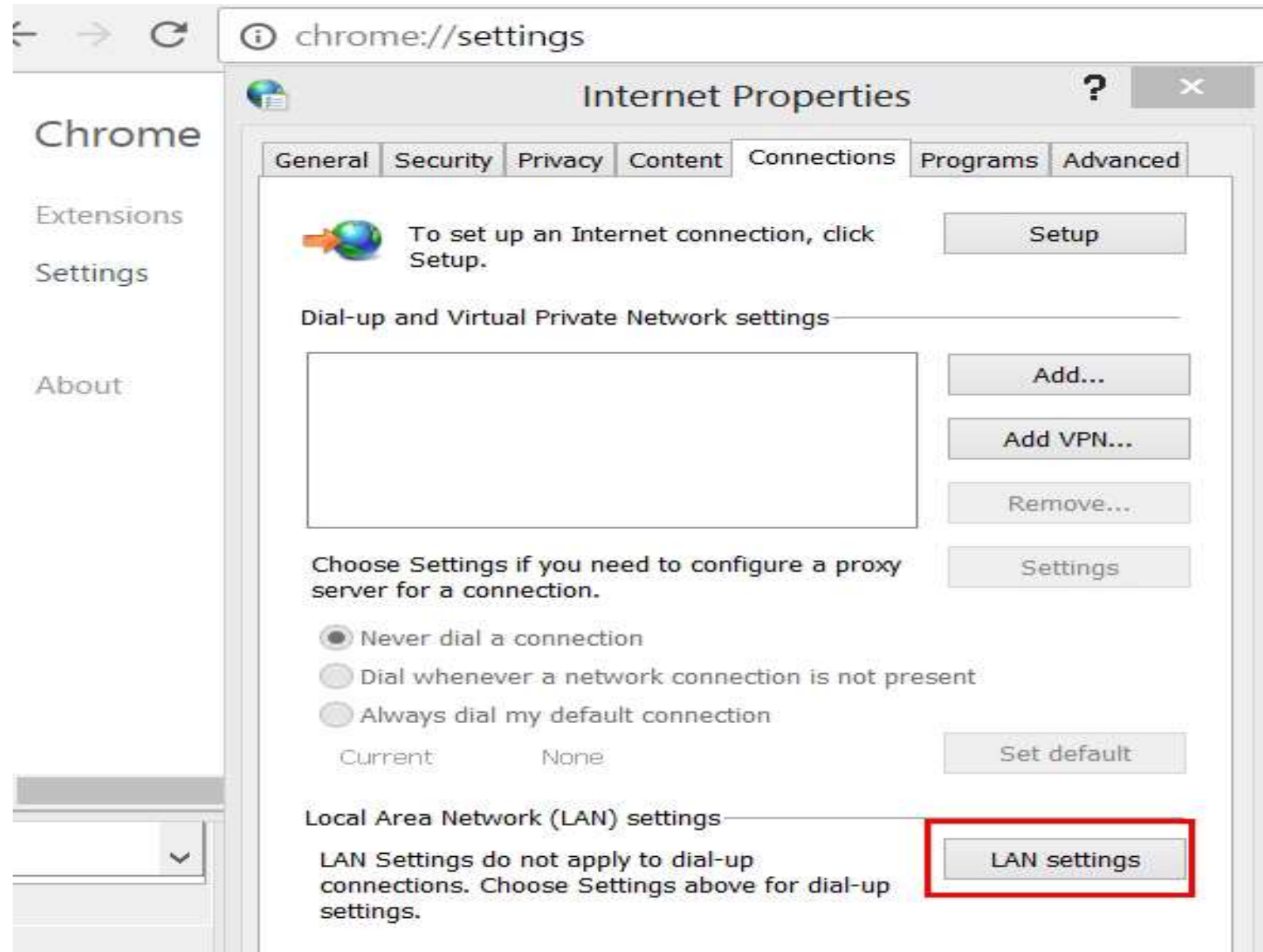


# Proxy Server Setting Chrome Browser



The screenshot shows the Chrome browser settings page. The address bar displays "chrome://settings". The left sidebar contains navigation options: Chrome, Extensions, Settings, and About. The main content area is titled "Settings" and includes sections for "Page zoom" (set to 100%), "Network", and "Languages". In the "Network" section, a message states "Google Chrome is using your computer's system proxy settings" and a button labeled "Change proxy settings..." is highlighted with a red rectangular box. Below this, the "Languages" section is partially visible, showing a button for "Language and input settings..." and a checked checkbox for "Offer to translate pages that aren't in a language you".

# Proxy Server Setting Chrome Browser



The image shows a Chrome browser window with the address bar displaying "chrome://settings". The "Settings" page is open, and the "Internet Properties" dialog box is overlaid on top. The "Connections" tab is selected in the dialog box. The "LAN settings" button is highlighted with a red rectangle.

chrome://settings

Internet Properties

General Security Privacy Content Connections Programs Advanced

To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

Add... Add VPN... Remove... Settings

Choose Settings if you need to configure a proxy server for a connection.

Never dial a connection  
 Dial whenever a network connection is not present  
 Always dial my default connection

Current None Set default

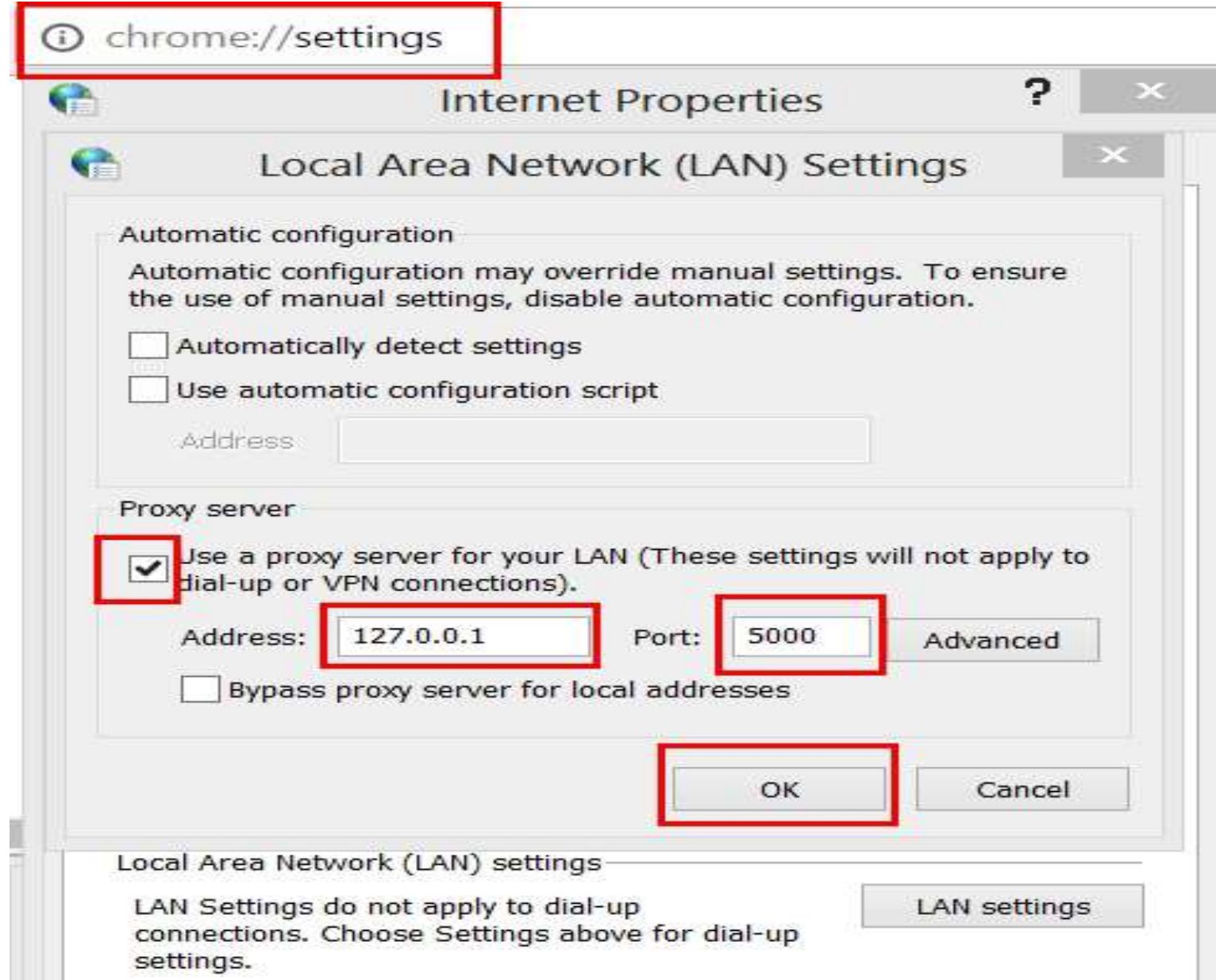
Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

LAN settings



# Proxy Server Setting Chrome Browser



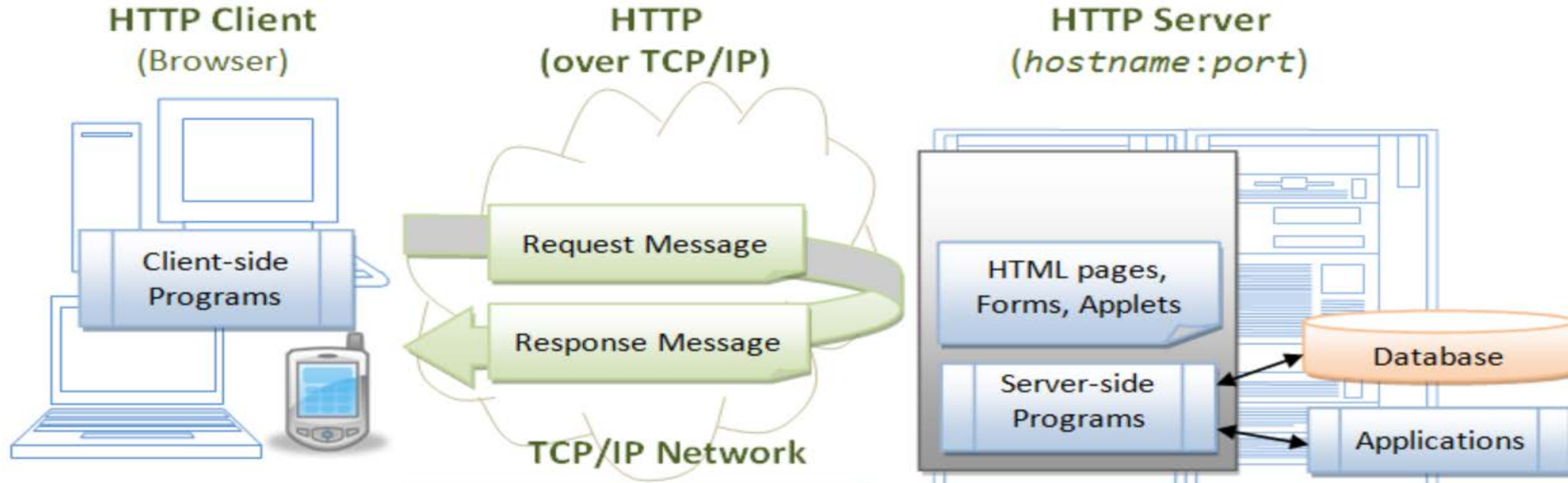
# Setting Paros Local Proxy : Tools >> Options >> Local Proxy

The screenshot shows the Paros Proxy application window titled "Untitled Session - Paros". The "Tools" menu is open, and the "Options..." option is selected. The "Options" dialog box is displayed, showing a tree view on the left with "Local proxy" selected. The "Local proxy" section on the right contains the following settings:

- Local proxy
- Address (eg localhost, 127.0.0.1): localhost
- Port (eg 8080): 5000

Below the input fields, a text box contains the instruction: "Set your browser proxy setting using the above. The http port and https port must be the same port as above." The dialog box has "OK" and "Cancel" buttons at the bottom right.

# Web Port Number → Jump to Pertinent Service Program



Application	<b>HTTP</b>
Presentation	SSL
Session	
Transport	<b>TCP</b>
Network	<b>IP</b>
Data Link	IEEE 802.11x
Physical	

Multiplexing (Port), Re-transmission Addressing (IP Address), Routing





## Web Port Number(16bits-64k) → Assigned Service Handler

**IANA:  
Internet Assigned  
Numbers Authority**

Label on Column	Service Name	UDP and TCP Port Numbers Included
DNS	Domain Name Service – UDP	UDP 53
DNS TCP	Domain Name Service – TCP	TCP 53
HTTP	Web	TCP 80
HTTPS	Secure Web (SSL)	TCP 443
SMTP	Simple Mail Transport	TCP 25
POP	Post Office Protocol	TCP 109, 110
SNMP	Simple Network Management	TCP 161,162 UDP 161,162
TELNET	Telnet Terminal	TCP 23
FTP	File Transfer Protocol	TCP 20,21
SSH	Secure Shell (terminal)	TCP 22
AFP IP	Apple File Protocol/IP	TCP 447, 548

## Paros Scanning

**HTTP Request**  
**HTTP Response**

**Crawl Structure**

**Header part**

**Body part**

**Crawl Information URL/URI Web Log Information**

Google - Microsoft Internet Explorer  
주소 http://www.google.co.kr/

Untitled Session - Paros  
File Edit View Analyse Report Tools Help

Sites  

- http://www.google.co.kr
  - GET:ads
  - GET:advanced\_search(hl)**
  - GET:favicon.ico
  - GET:ig
  - GET:jobs
  - GET:language\_tools(hl)
  - GET:options
  - GET:preferences(hl)
  - GET:url(pref.pval.q.sa)
  - ig

Request Response Trap  
GET http://www.google.co.kr/advanced\_search?hl=ko HTTP/1.1  
Host: www.google.co.kr  
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0;) Paros/3.2.13  
Pragma: no-cache  
Content-Type: application/x-www-form-urlencoded  
Referer: http://www.google.co.kr  
Content-length: 0

URI found during crawl:  
http://www.google.co.kr/support/jobs/bin/answer.py?answer=65022  
http://www.google.co.kr/support/jobs/bin/answer.py?answer=65482  
http://www.google.co.kr/intl/ko/privacy.html

URI found but out of crawl scope:  
http://translate.google.co.kr/translate\_s?hl=ko&q=&sl=nl&tl=nl  
http://translate.google.co.kr/translate\_t  
http://translate.google.co.kr/translate\_s  
http://translate.google.co.kr/translate\_t?langpair=  
http://translate.google.co.kr/translate

History Spider Alerts Output

# Paros modify HTTP Data

A Simple Form with JavaScript Validation - Microsoft Internet Explorer

파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도구(T) 도움말(H)

주소(D) http://www.elated.com/res/File/articles/development/javascript/form-validation-with-javascript

Cookie Proxy: (none) Typed URLs Visited URLs Cache Passwo

## Please Enter Your Name

Your Name:

Send Details

**Microsoft Internet Explorer**

Please fill in the 'Your Name' box.

확인

완료

simple\_form[1] - 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```

<head>
<title>A Simple Form with JavaScript Validation</title>
<script type="text/javascript">
<!--
Function validate_form ( )
{
    valid = true;

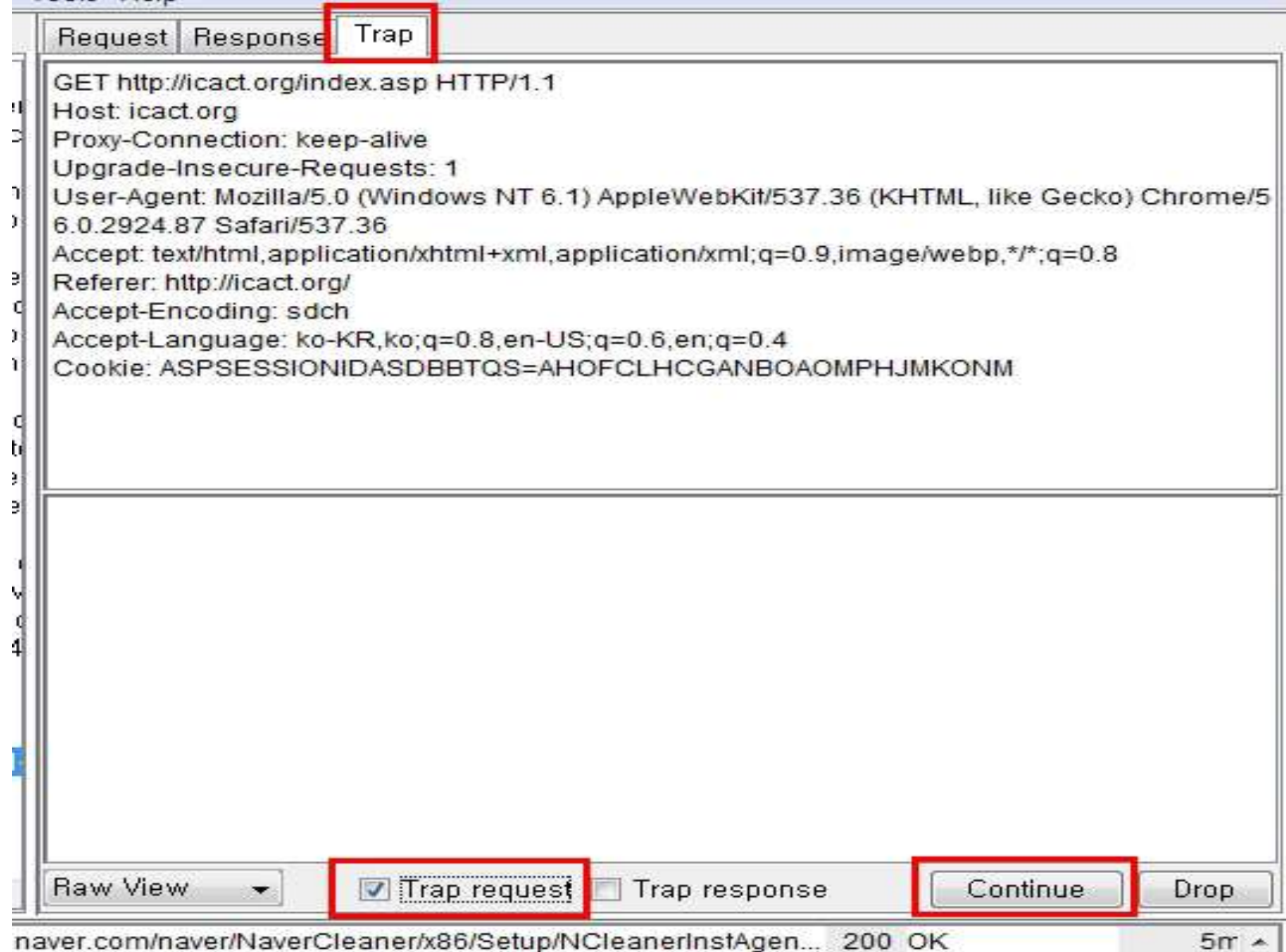
    if ( document.contact_form.contact_name.value == "" )
    {
        alert ( "Please fill in the 'Your Name' box." );
        valid = false;
    }

    return valid;
}
//-->

```



# Paros intercept & modify HTTP Data



Request Response **Trap**

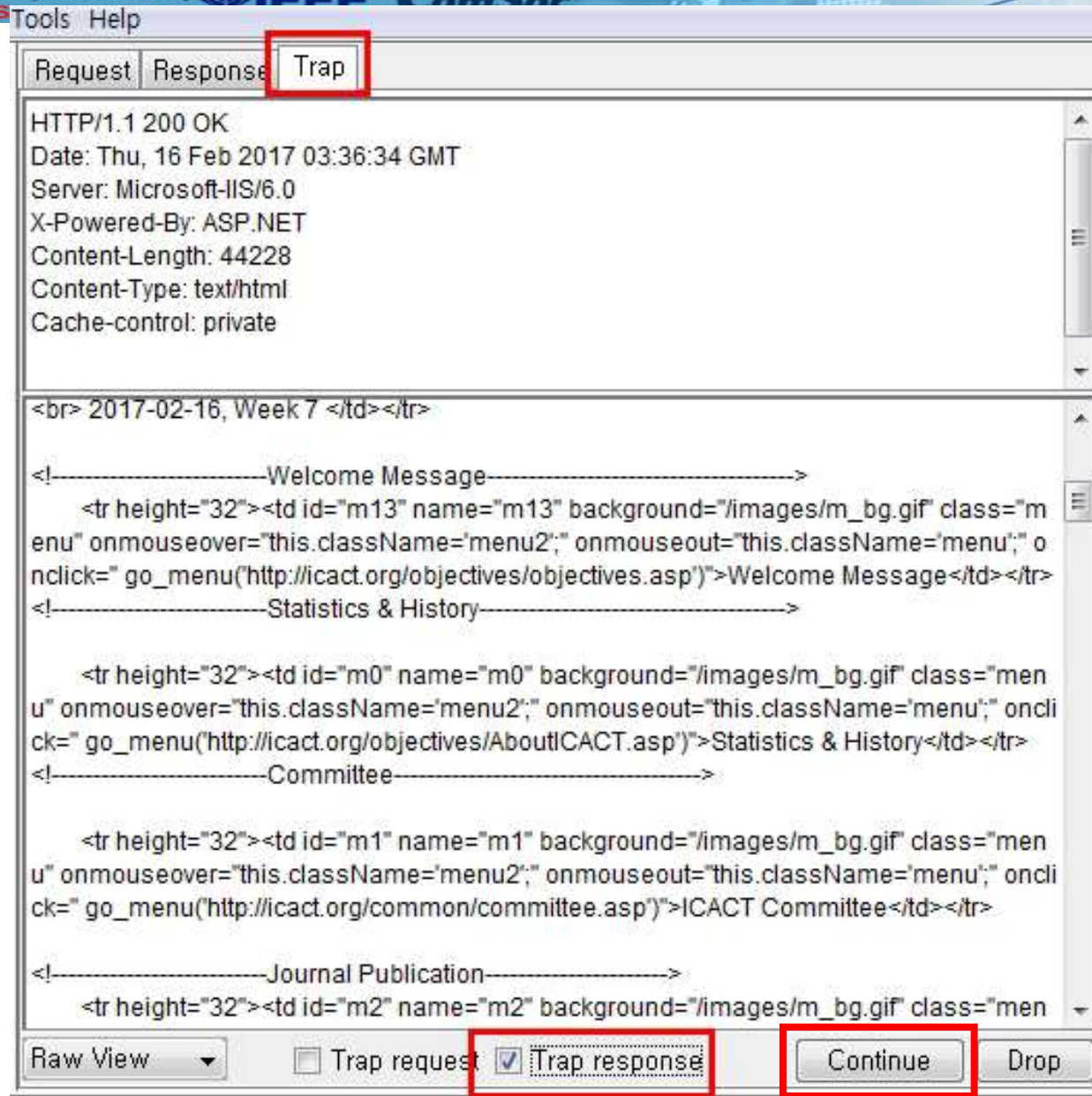
```

GET http://icact.org/index.asp HTTP/1.1
Host: icact.org
Proxy-Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://icact.org/
Accept-Encoding: sdch
Accept-Language: ko-KR,ko;q=0.8,en-US;q=0.6,en;q=0.4
Cookie: ASPSESSIONIDASDBBTQS=AHOFCLHCGANBOAOMPJMKONM
    
```

Raw View  **Trap request**  Trap response **Continue** Drop

naver.com/naver/NaverCleaner/x86/Setup/NCleanerInstAgen... 200 OK 5m

# Paros intercept & modify HTTP Data



Tools Help

Request Response **Trap**

```

HTTP/1.1 200 OK
Date: Thu, 16 Feb 2017 03:36:34 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Content-Length: 44228
Content-Type: text/html
Cache-control: private

```

```

<br> 2017-02-16, Week 7 </td></tr>

<!-------Welcome Message----->
  <tr height="32"><td id="m13" name="m13" background="/images/m_bg.gif" class="m
enu" onmouseover="this.className='menu2';" onmouseout="this.className='menu';" o
nclick=" go_menu('http://icact.org/objectives/objectives.asp')>Welcome Message</td></tr>
<!-------Statistics & History----->

  <tr height="32"><td id="m0" name="m0" background="/images/m_bg.gif" class="men
u" onmouseover="this.className='menu2';" onmouseout="this.className='menu';" oncli
ck=" go_menu('http://icact.org/objectives/AboutICACT.asp')>Statistics & History</td></tr>
<!-------Committee----->

  <tr height="32"><td id="m1" name="m1" background="/images/m_bg.gif" class="men
u" onmouseover="this.className='menu2';" onmouseout="this.className='menu';" oncli
ck=" go_menu('http://icact.org/common/committee.asp')>ICACT Committee</td></tr>

<!-------Journal Publication----->
  <tr height="32"><td id="m2" name="m2" background="/images/m_bg.gif" class="men

```

Raw View  Trap request  Trap response **Continue** Drop

## Paros Demonstration !

[http://www.skku.edu/index\\_pc.jsp](http://www.skku.edu/index_pc.jsp) >>global

[http://www.skku.edu/eng\\_home/index.jsp](http://www.skku.edu/eng_home/index.jsp)

GET <http://admission-global.skku.edu/admission/about/welcome.jsp>  
HTTP/1.1

GET <http://admission-global.skku.edu/admission/undergraduate/schedule.jsp> HTTP/1.1

Hack

<http://admission-global.skku.edu/admission/about/contact.jsp>

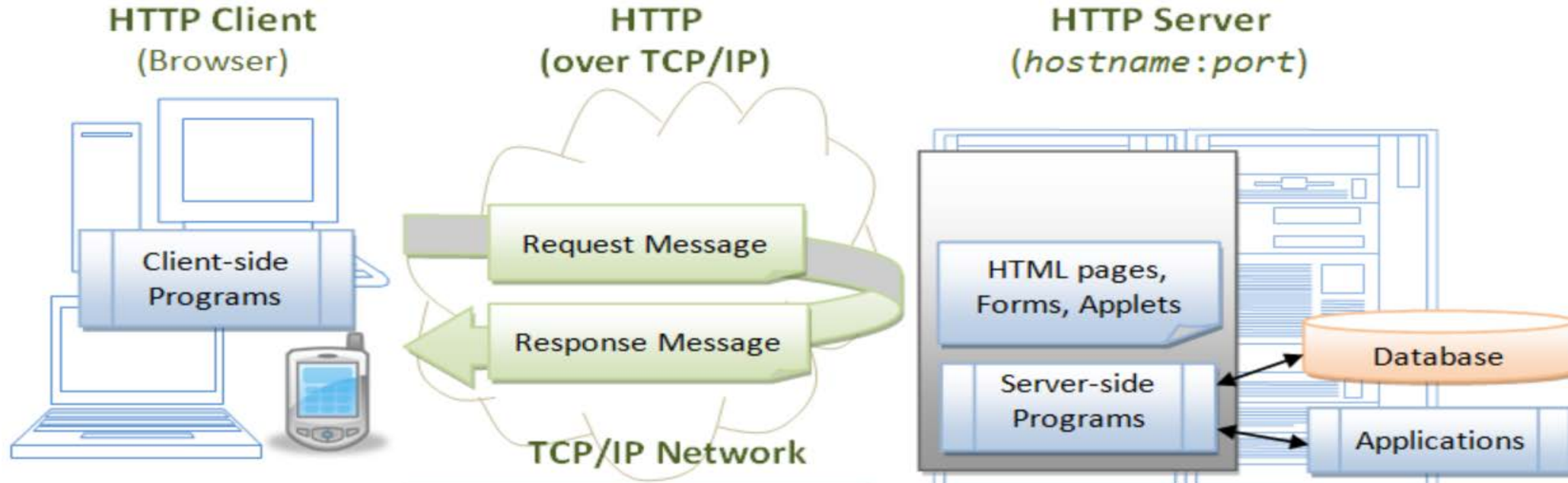




# Wrap Up!

1. Stateless Web Programming
2. Cookie
3. HTTP GET and POST Method
4. Paros Proxy Server Capability

# WWW Web Service Overview – Look Around !



Application	<b>HTTP</b>
Presentation	SSL
Session	
Transport	<b>TCP</b>
Network	<b>IP</b>
Data Link	IEEE 802.11x
Physical	

Multiplexing (Port), Re-transmission Addressing (IP Address), Routing



# Web Hacking & Defensing! - OWASP top 10 vulnerabilities

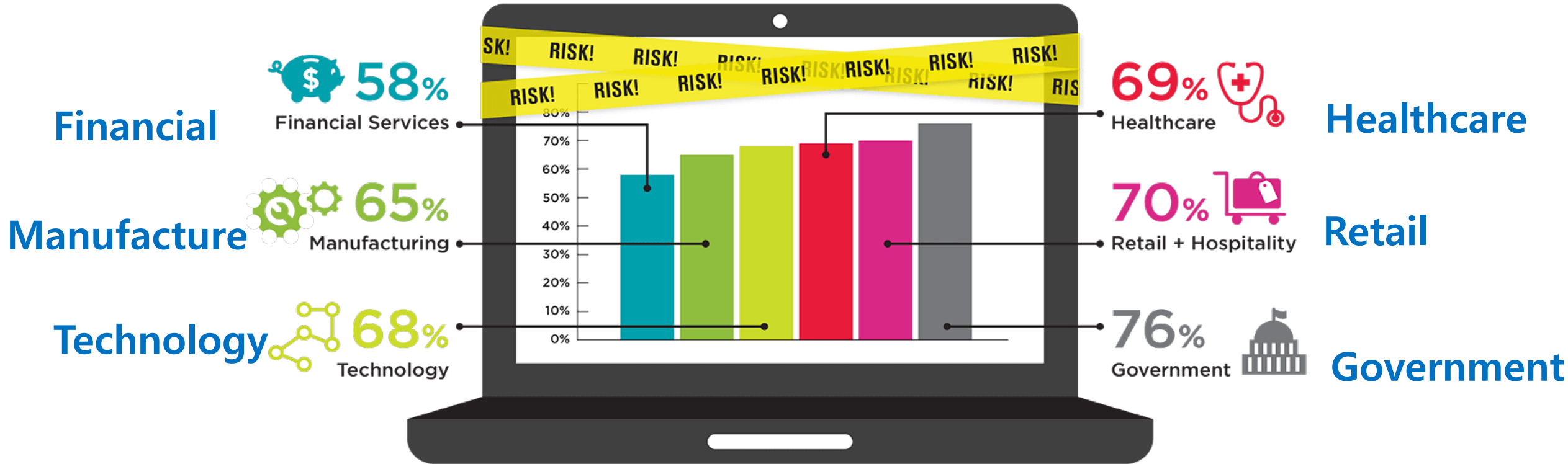
**OWASP : Open Web Application Security Project**

- #1 **SQL Injection**
- #2 **Broken Authentication and Session Management**
- #3 **XSS: Cross-Site Scripting**
- #4 **Insecure direct object reference**
- #5 **Security misconfiguration**
- #6 **Sensitive data exposure**
- #7 **Missing function level access control**
- #8 **Cross-site request forgery**
- #9 **Using components with known vulnerabilities**
- #10 **Invalidated redirects and forwards**



# FAILED OWASP TOP 10

How many apps fail the OWASP Top 10 upon initial risk assessment?



The data represents 208,670 application assessments submitted for analysis during the 18-month period from October 1, 2013 through March 31, 2015 by large and small companies, commercial software suppliers, open source projects and software outsourcers.