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

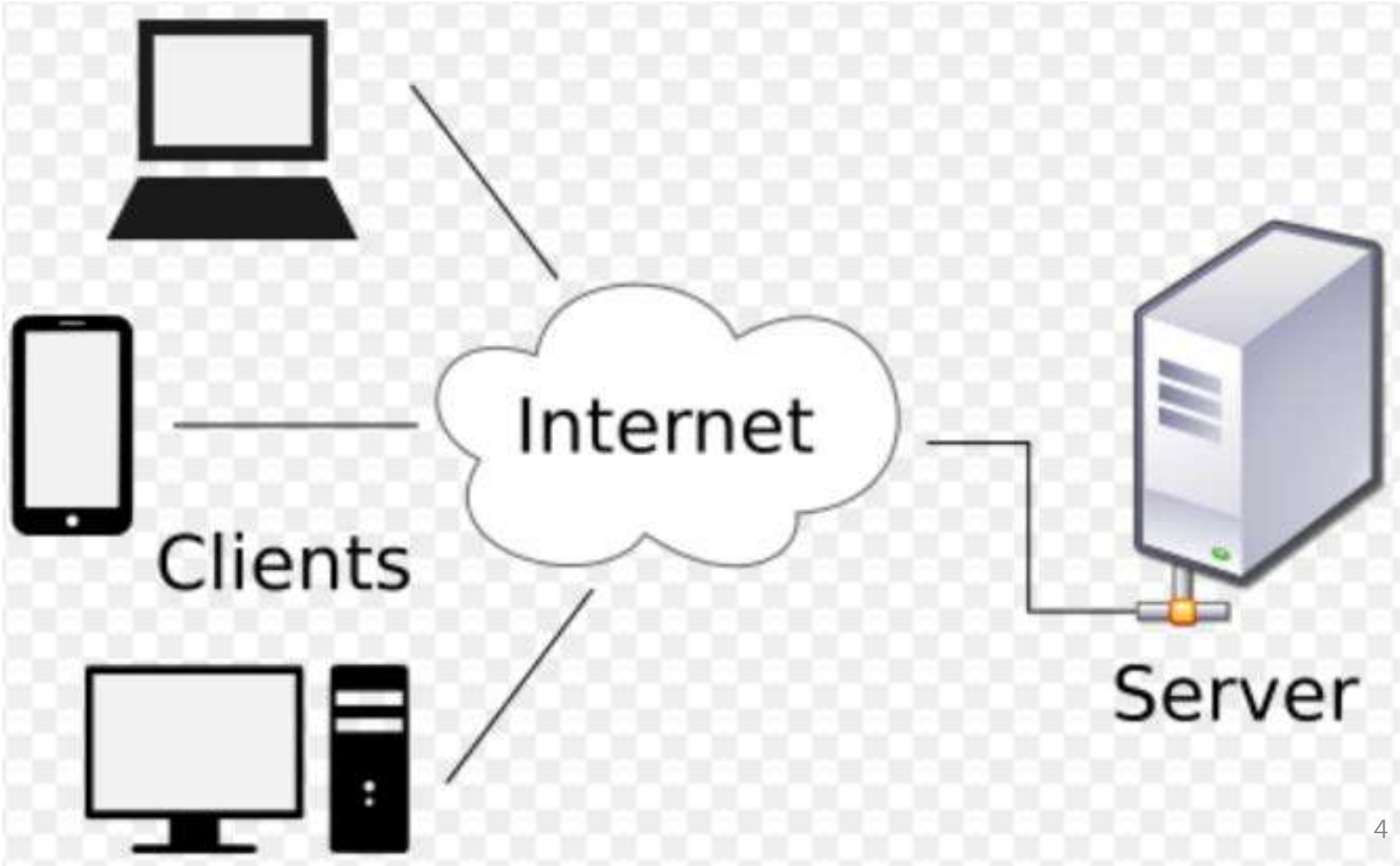
3. Web Log Analysis

   – Fundamental Knowledge of Hacking Type Analysis

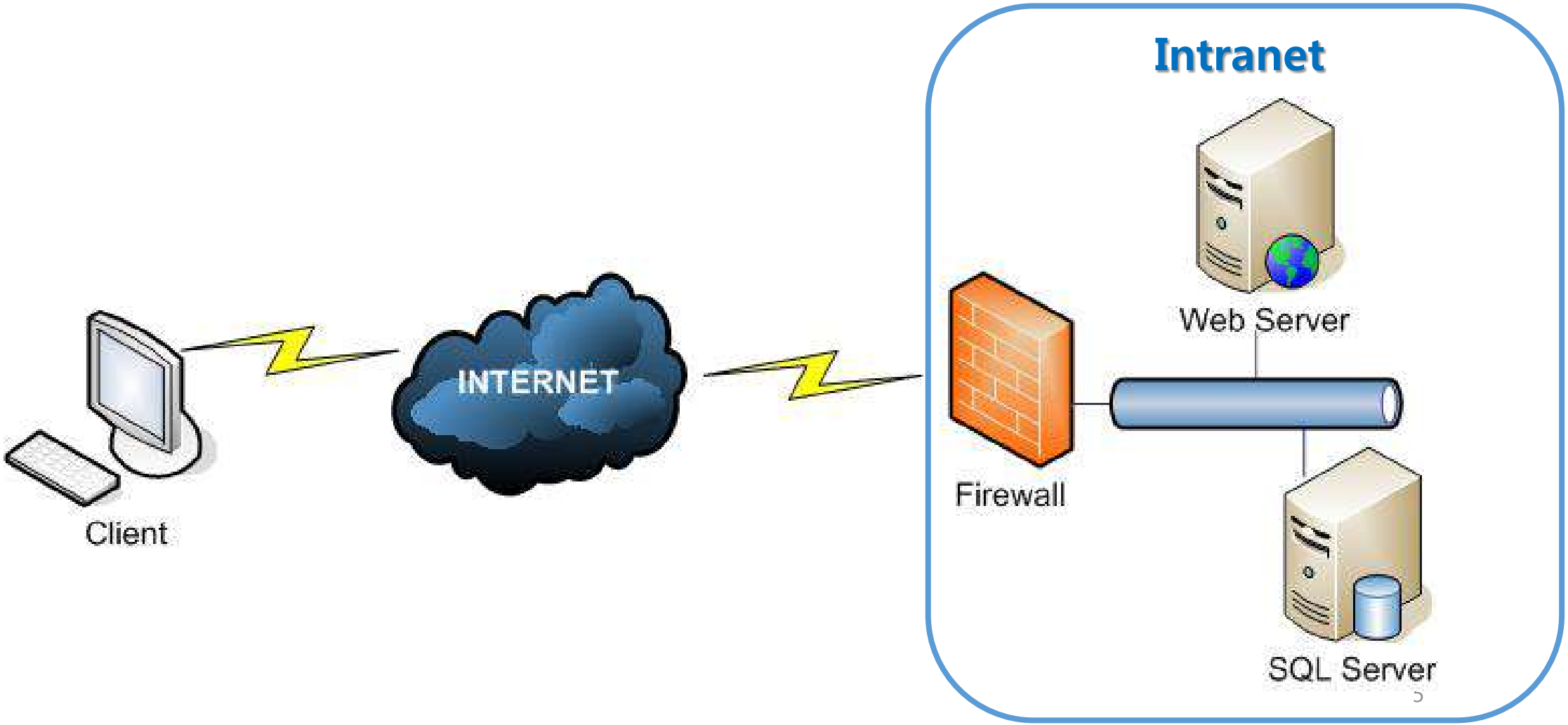
4. Web Defensing Know-How

   - Become a Cyber Soldier – Cyber Salvation Army

Internet Logical Architecture → Cyber Space L.A.

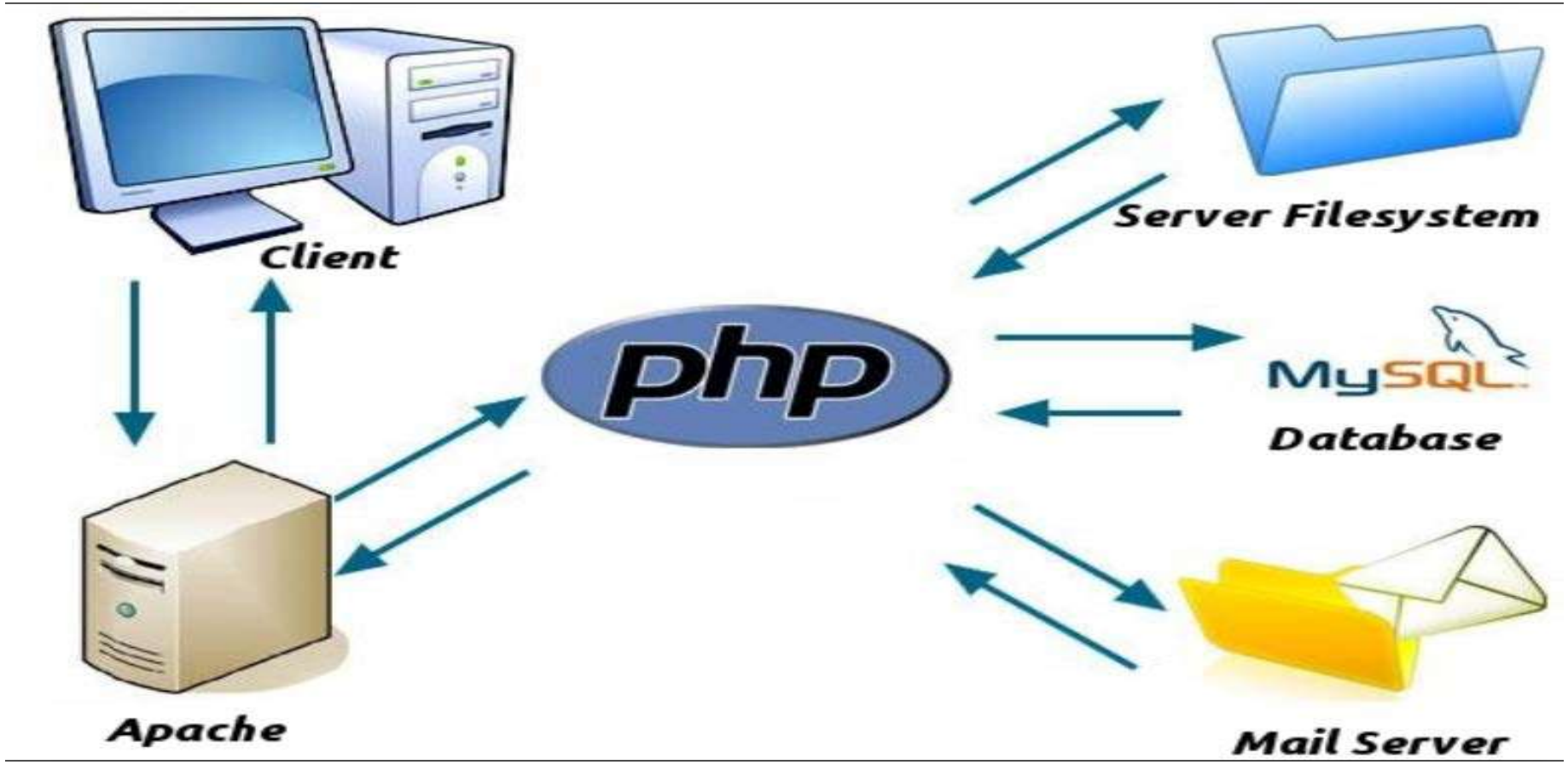


Intranet Logical Architecture



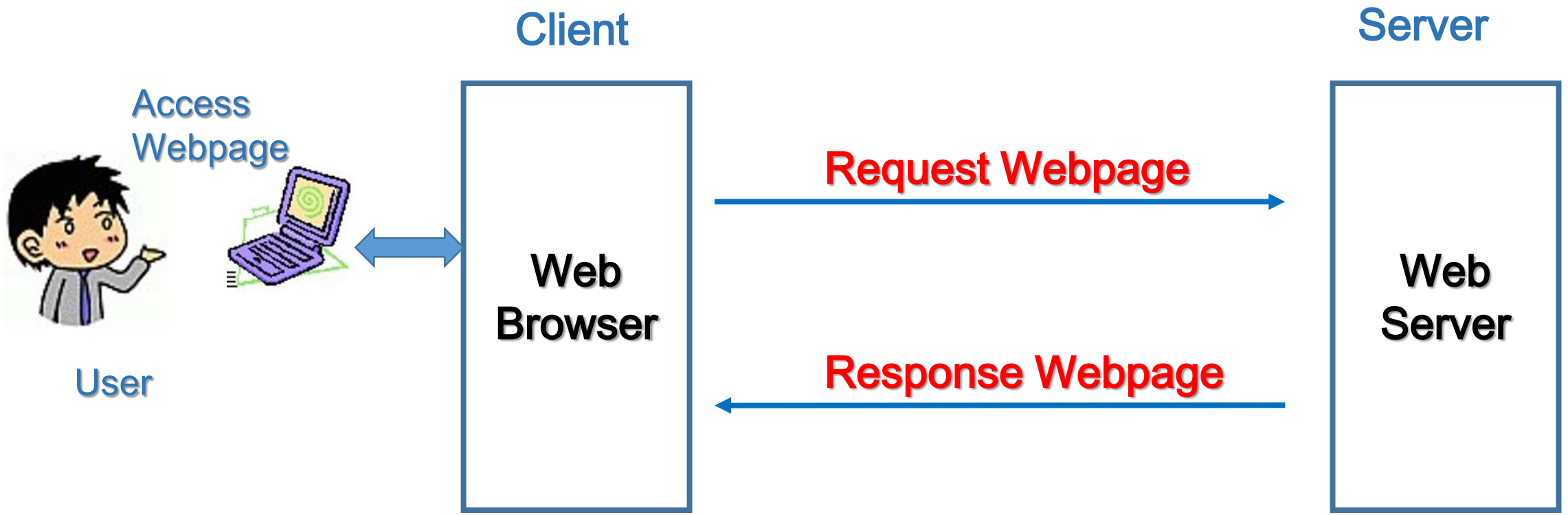
Web Server Platform – Web Programming Environment

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)



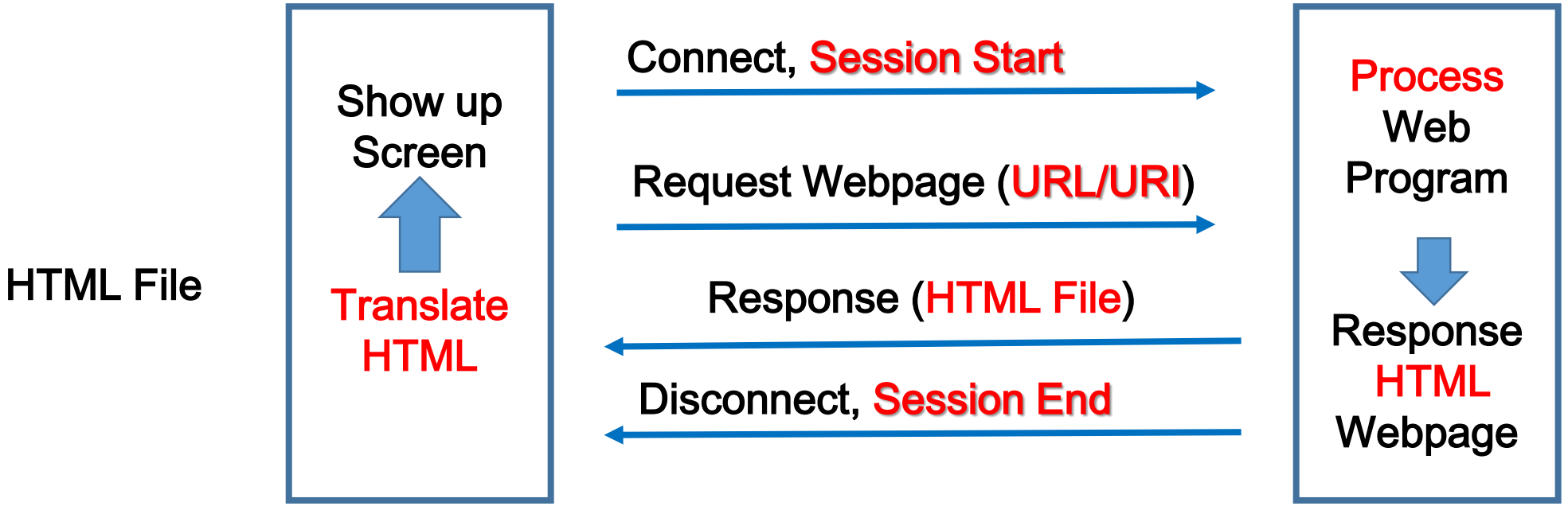
Cyber Space Protocol – HTTP (Hyper Text Transport Protocol)

1. Web Browser request Webpage

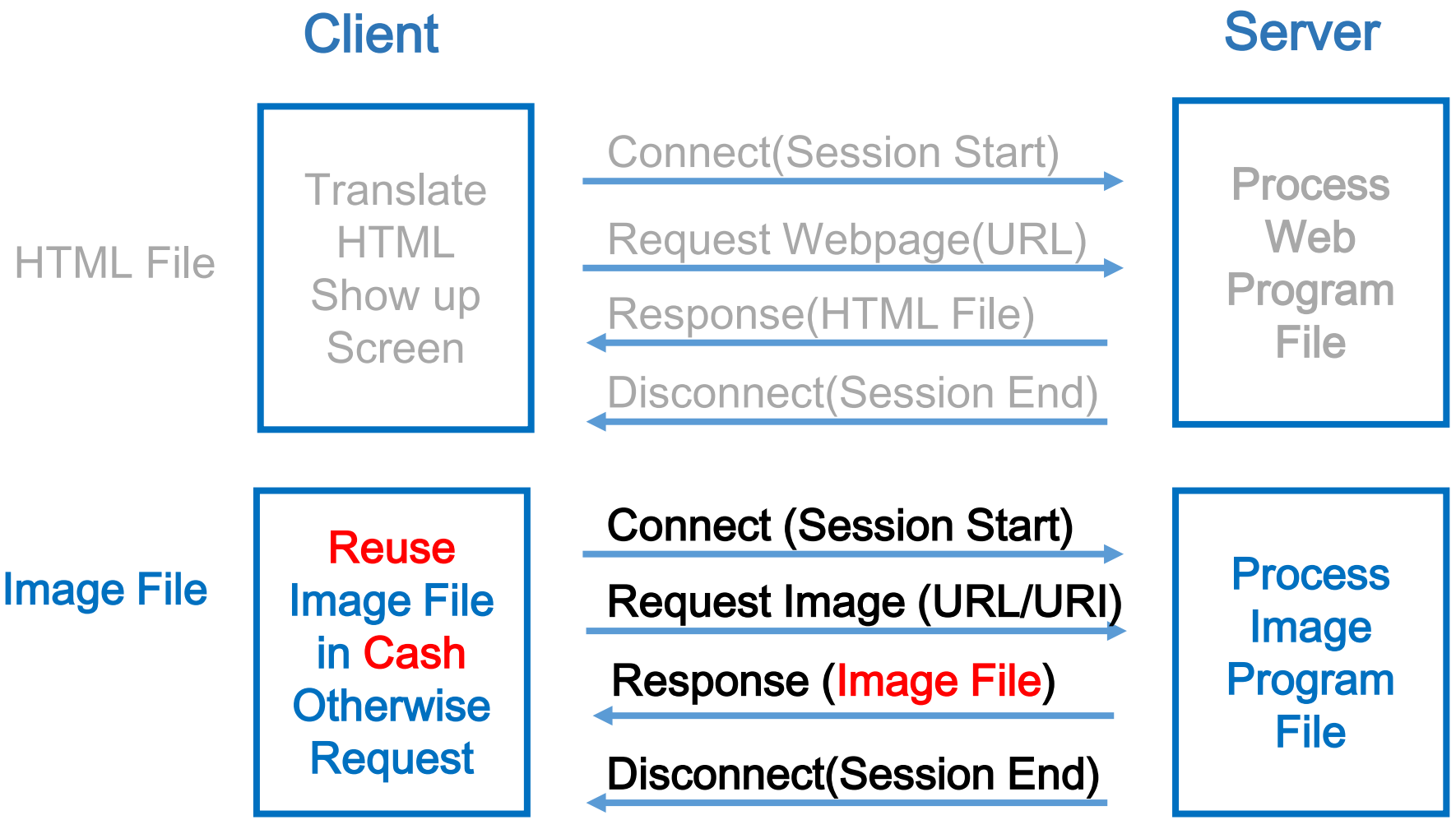
2. Server Process

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 Instances

→ HTML5, CSS, …

→Server-side Program : ASP, JSP, PHP, …

→SQL DBMS Language

→ Embedded Multi-Media Languages

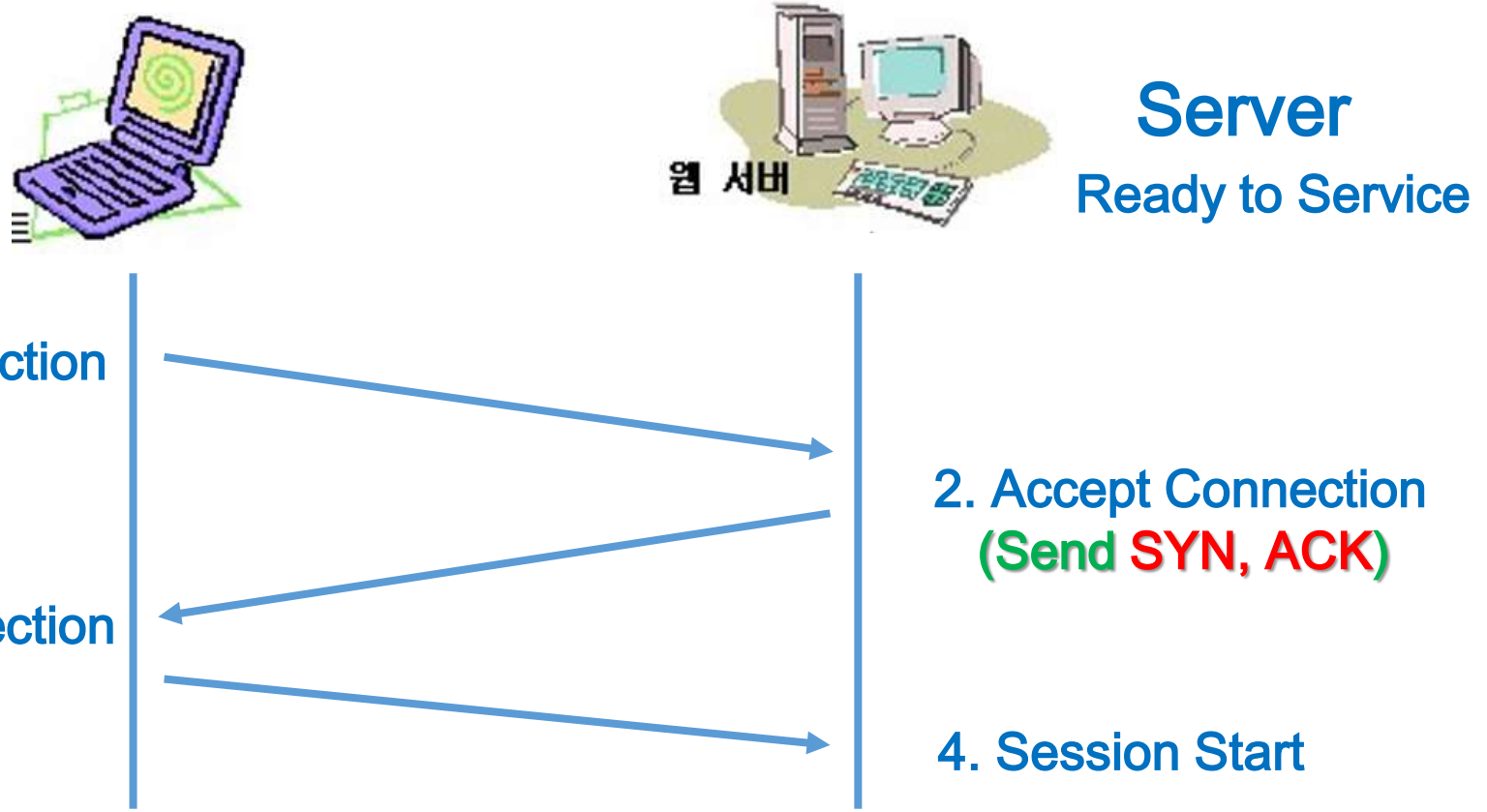
: Audio, Video, Image, Streaming Service

: File Upload, Download

: Send & Receive eMail

: CSV, Excel file between DBMS, … etc.

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



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)

Ready to service

2. TCP Checksum Routine
(Send ACK)

3. Give Webpage
(document-PSH)

4. TCP Checksum Routine
(send ACK)

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

2. CLOSE-WAIT
(send ACK)

3. FIN-WAIT 2

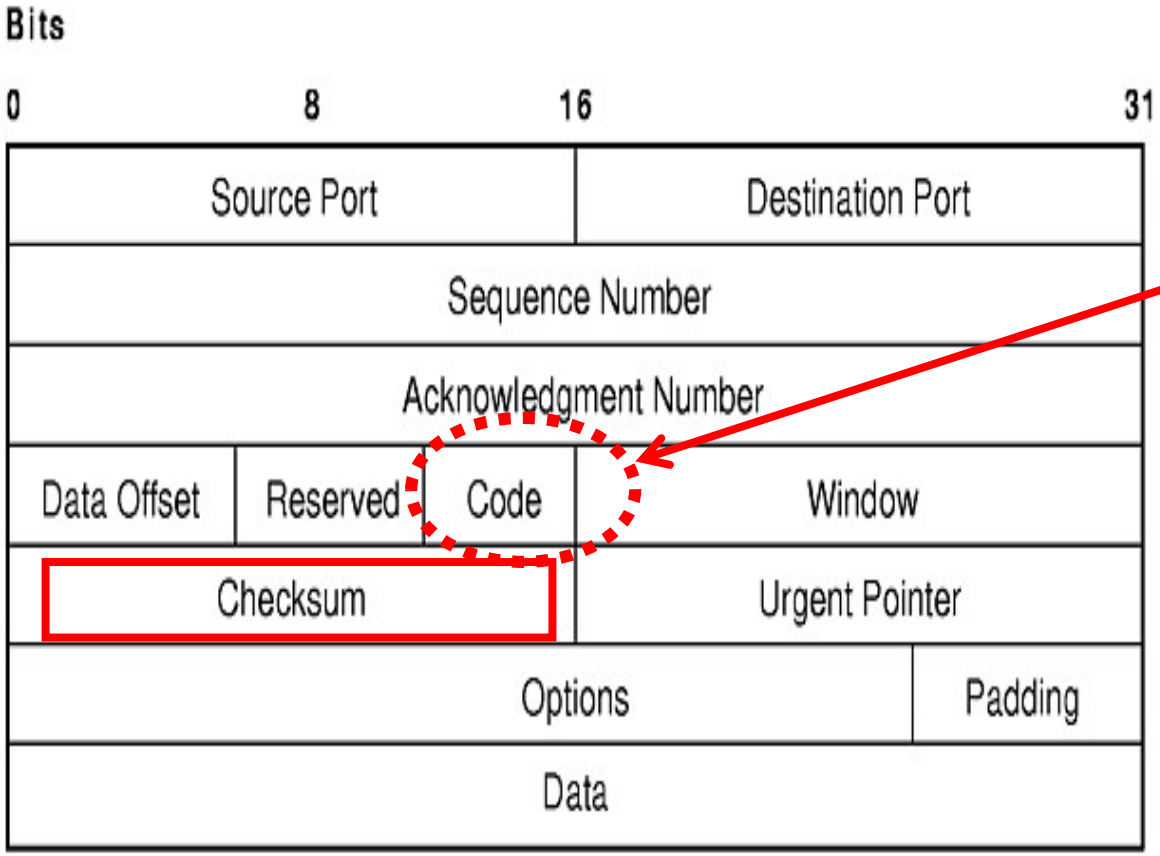
4. LAST ACK
(Send FIN, ACK)

5. TIME WAIT
(send ACK)

6. Session End

Global Client-Server Communication Protocol

Cyber Space Protocol –TCP Date lossless Protocol Packet Format

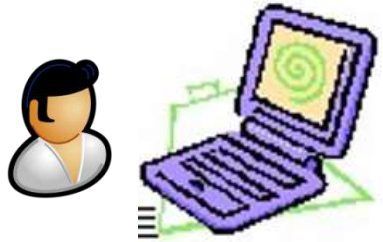


Transmission Control Protocol (TCP) Packet Header

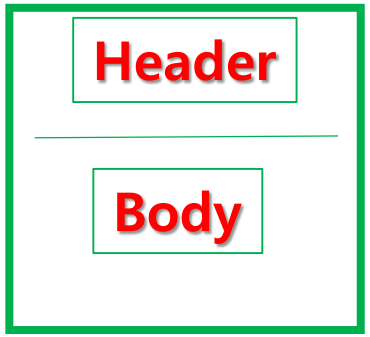
Code - Flag Bits
(Packet Control Code)

- **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

Cyber Space Protocol – HTTP Request & Response Message Format



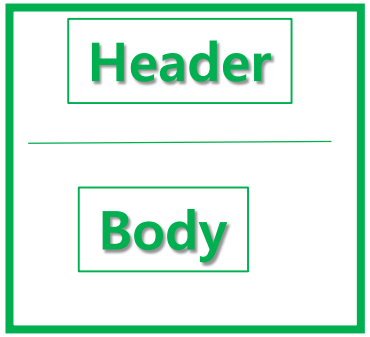
HTTP Request Message



User (Browser)

Web Server

HTTP Response Message



Cyber Space Protocol – HTTP Request Message Format

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 Massage

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

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

← HTTP Method

Massage Header Part

Massage 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

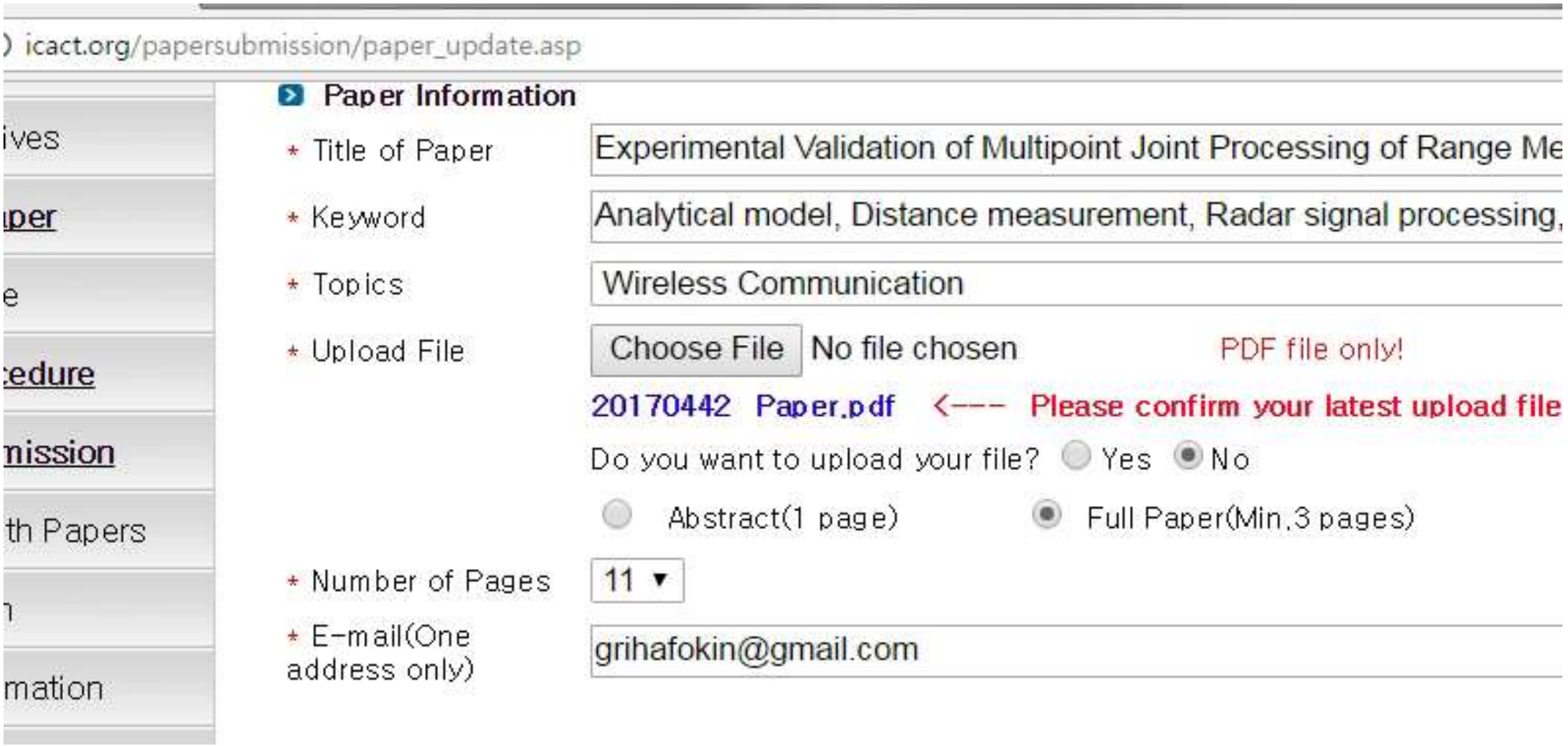
Cyber Space Protocol – HTTP Post Method Request Method

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

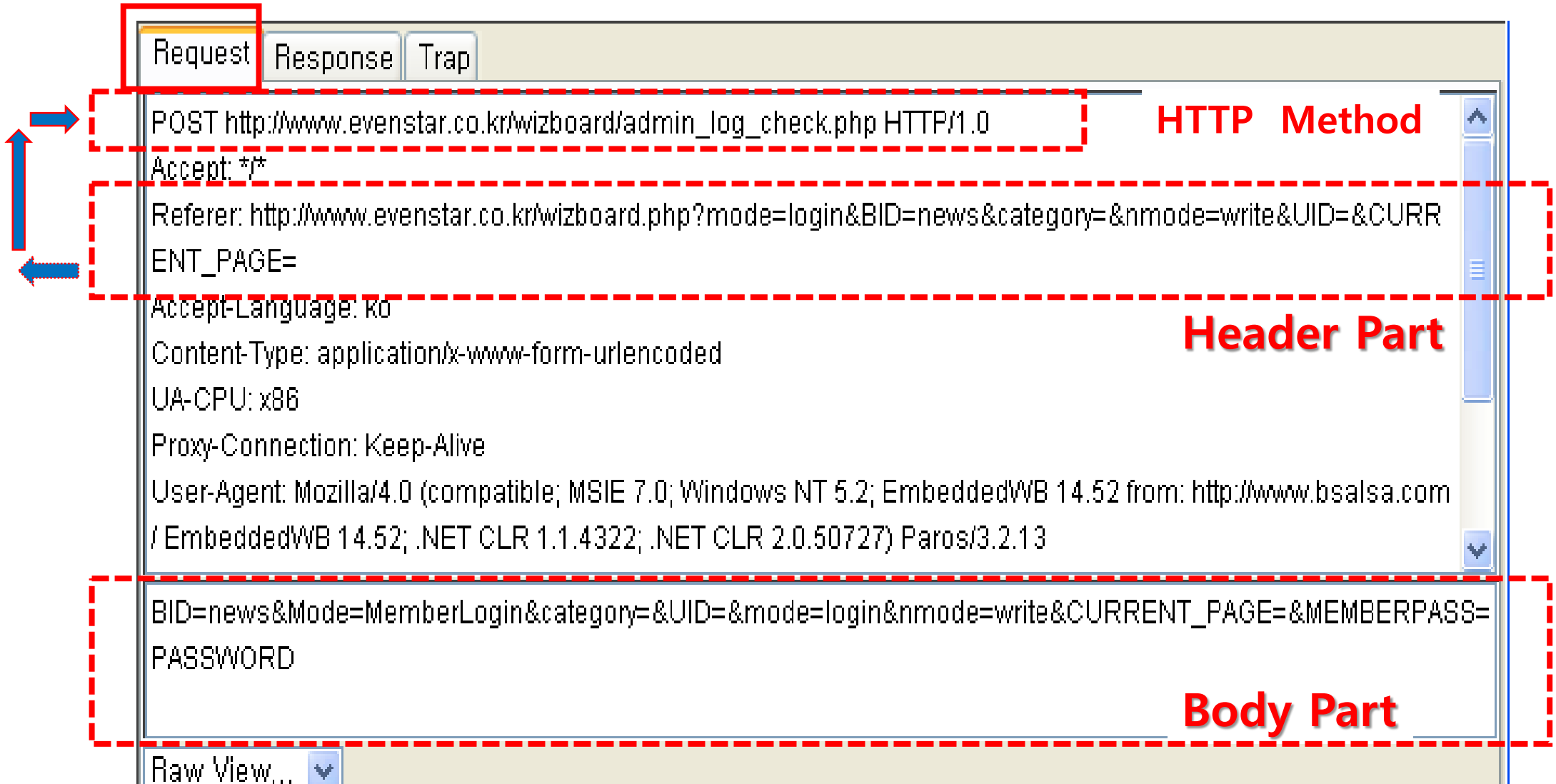
Method	Format	Note
POST	POST [request-uri] HTTP/1.1 Host:[Hostname] or [IP] Content-Length:[Bytes] Content-Type:[Content Type] One White Space Line [query-string] or [Data]	1. Data Communication of Form Based Web Page with Various Data & Parameters. 2. Browser can't show up it at URL Window!

○ http://www.evenstar.co.kr/wizboard.php (http Header)
URI
BID=notice Query String (http Body)

Form based Webpage



Cyber Space Protocol – HTTP Post Method Request Message Scan



Form based Webpage HTTP Post Method Request Message Scan

Request | Response | Trap

```
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,ko;q=0.8,en-US;q=0.6,en;q=0.4
Cookie: ASPSESSIONIDAQBBBTQT=CCNNEPNACCPHCHOJJDAKAPOD

------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"
```

Header Part

Session(Cookie)

Body Part

Cyber Space Protocol – HTTP Response Massage 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

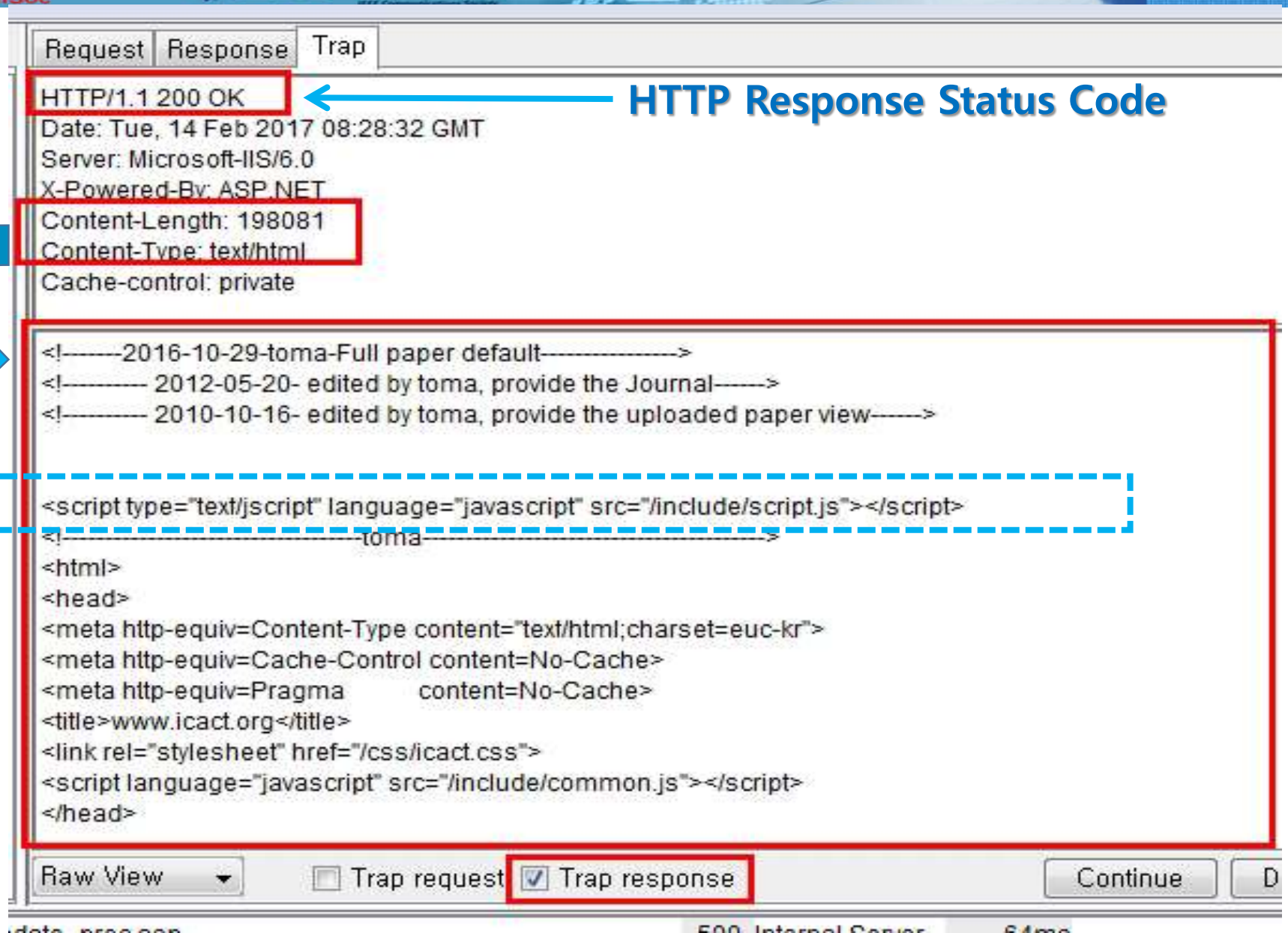
Header Part

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 Massage Scan



Form based Webpage

mission/paper_update.asp

Paper Information

* Title of Paper	Experimental Validation of Multipoint Joint Processing of Range Measurements v
* Keyword	Analytical model, Distance measurement, Radar signal processing, Radio naviga
* Topics	Wireless Communication
* Upload File	Choose File No file chosen PDF file only!

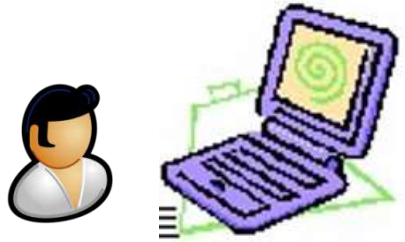
20170442 Paper.pdf <--- Please confirm your latest upload file here!

Do you want to upload your file? (•) Yes ( ) No

( ) Abstract(1 page) (•) Full Paper(Min.3 pages)

* Number of Pages	1
* E-mail(One address only)	grihafokin@gmail.com

Cyber Space Protocol – HTTP Response Status Code



Web Browser

Request(URL/URI)

Response(Status Code)

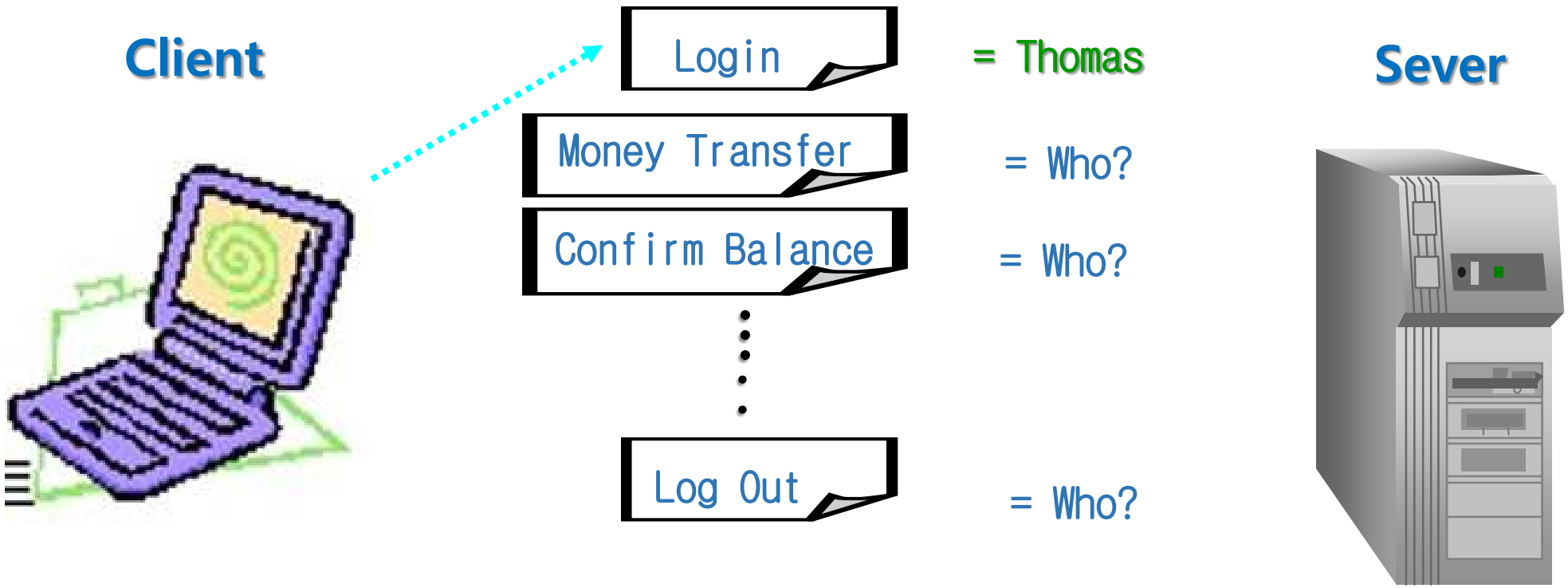
Web Server

- 200 : OK, Request Success
- 201 : File Created in Server
- 302 : Moved to Webpage (←Previous Webpage)
- 304 : Used Local Cache Info.
- 401 : Fail Authenticate
- 403 : Denied Access
- 404 : Not Exist Webpage
- 500 : Severe Error (DB Access Error ← Injection)

Cyber Space Web Programing Method – Stateless vs State Oriented

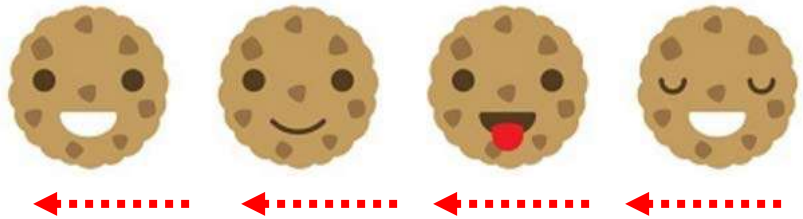
Cyber Space has Huge Users – Challenge & Chance

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

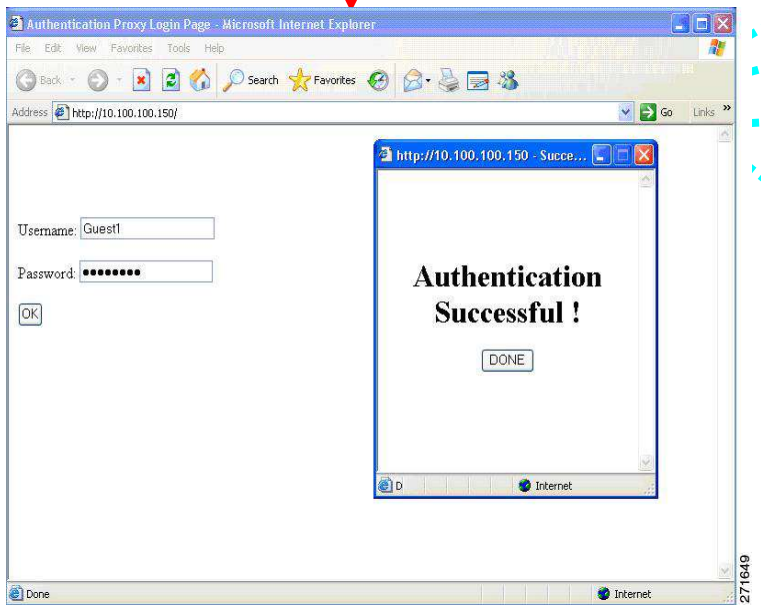


Banking Service Work Flow

Stateless Web Programing : Cookie



Client Keeps Cookie



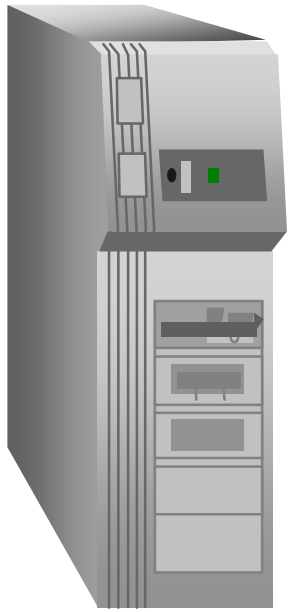
Login = Thomas

Money Transfer = Thomas

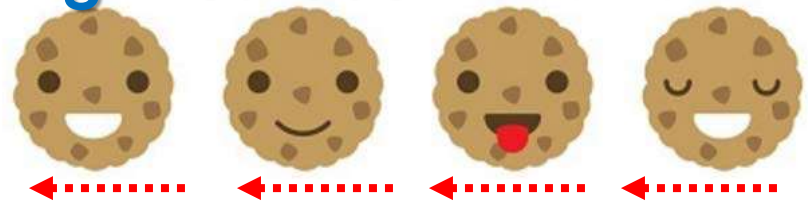
Confirm Balance = Thomas

Log Out = Thomas

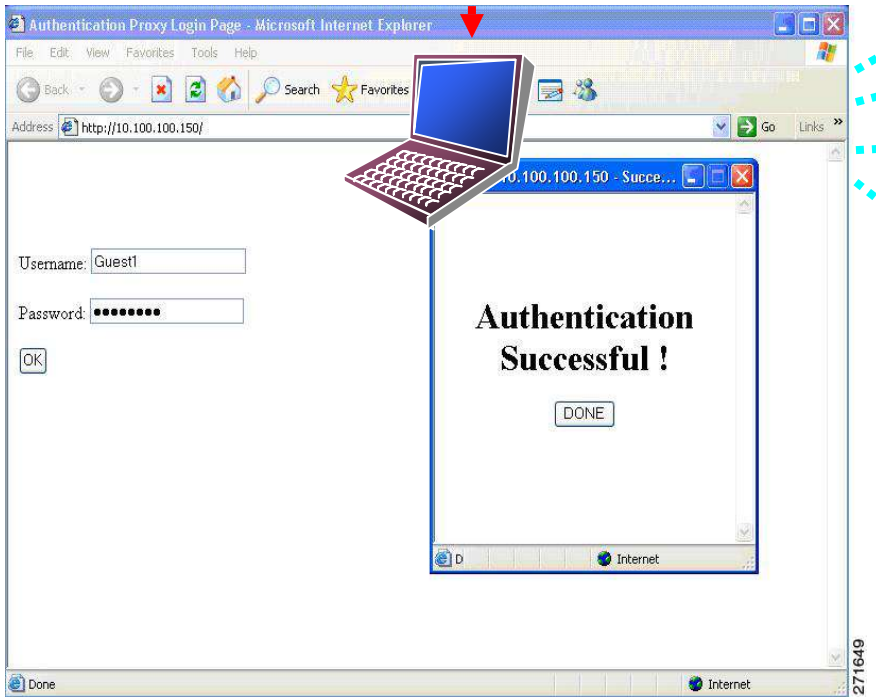
Server User Authenticate



Stateless Web Programing Methods : Cookie



Client Keeps Cookie



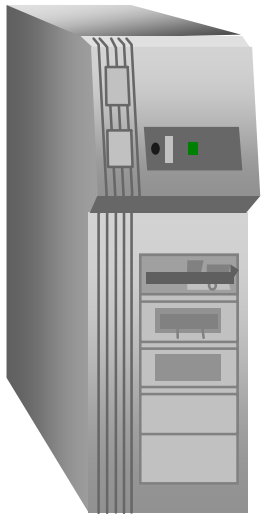
Login = Thomas

Money Transfer = Thomas

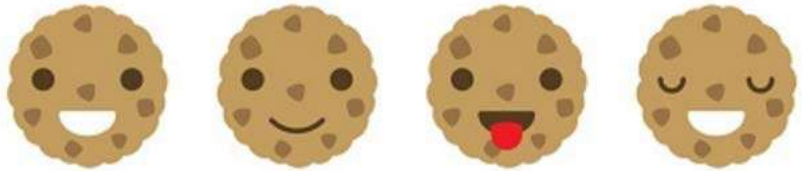
Confirm Balance = Thomas

Log Out = Thomas

Server User Authentication

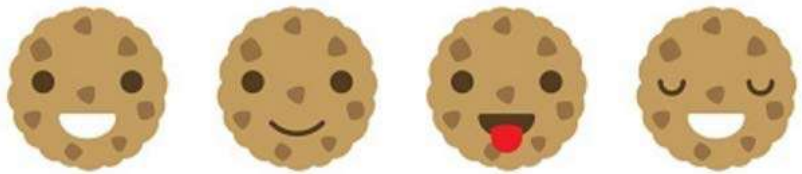


Stateless Web Programing Methods : Cookie



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

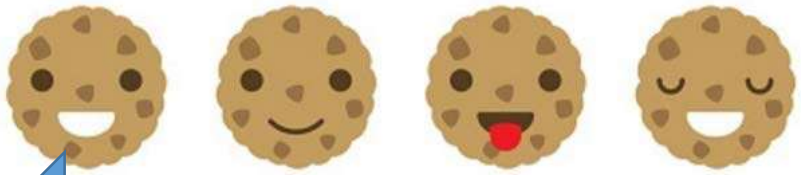
Stateless Web Programing Methods : Session Cookie Names



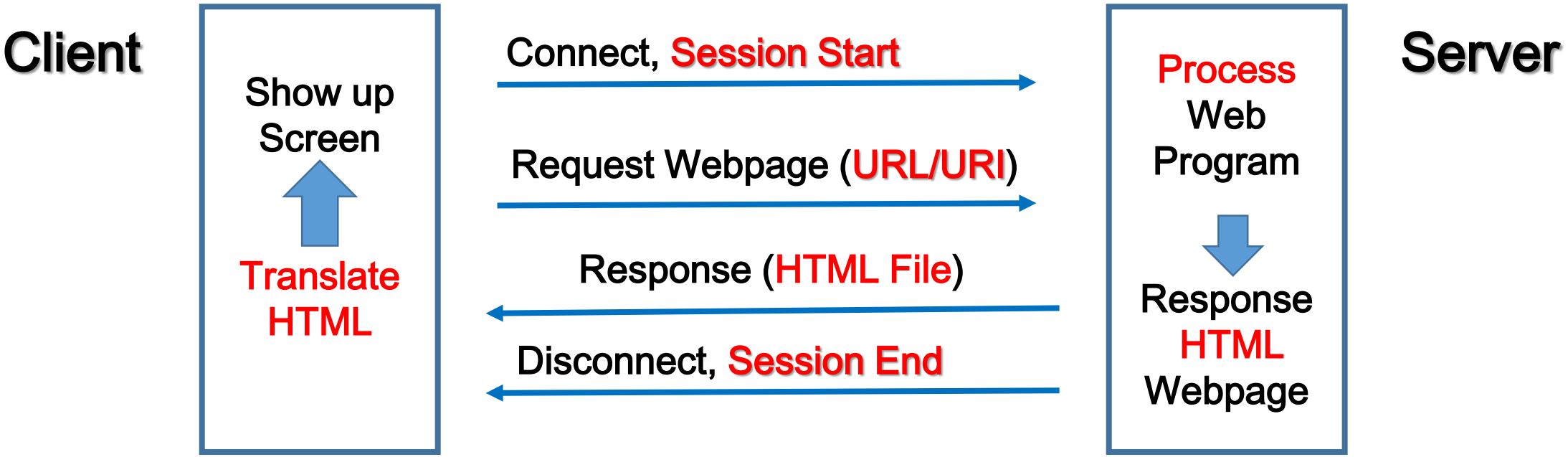
Hidden Parameter	Cookie	Session
Name, Password, Data	+UA	++Session ID
No Expire Time	Time-Out	Browser End
Very Simple	Secure	Very Secure
Store in Client	Store in Client	Critical Date in Server

Stateless Web Programing Methods : Cookie

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



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



Cookie Programing 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
```

```
<form name="frm" method="post">
 <input type="hidden" name="eMail" value="tomayoon@ieee.org">
 <input type="hidden" name="pwd" value="1111">
</form>

<script language="javascript">
<!--
        alert("tomayoon@ieee.org  Authentication Successful!  Go to the Annual Scheduler !");
        frm.action = "schedule.asp";
        frm.submit();
//-->
</script>
```

Raw View | ☐ Trap request | ☑ 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 Programing Methods : Cookie + Session ID

Untitled Session - Paros

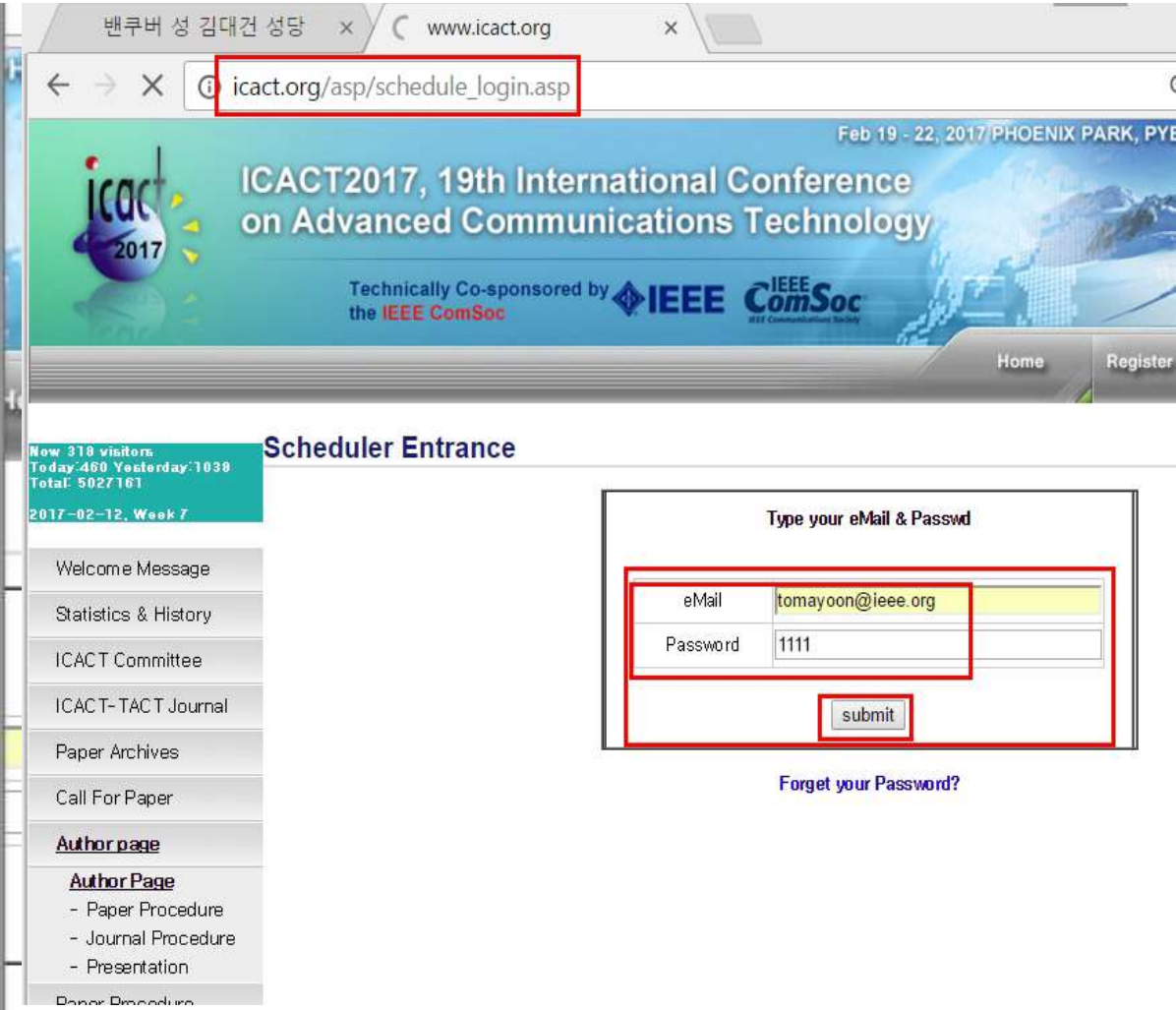
Report Tools Help

Request | Response | Trap

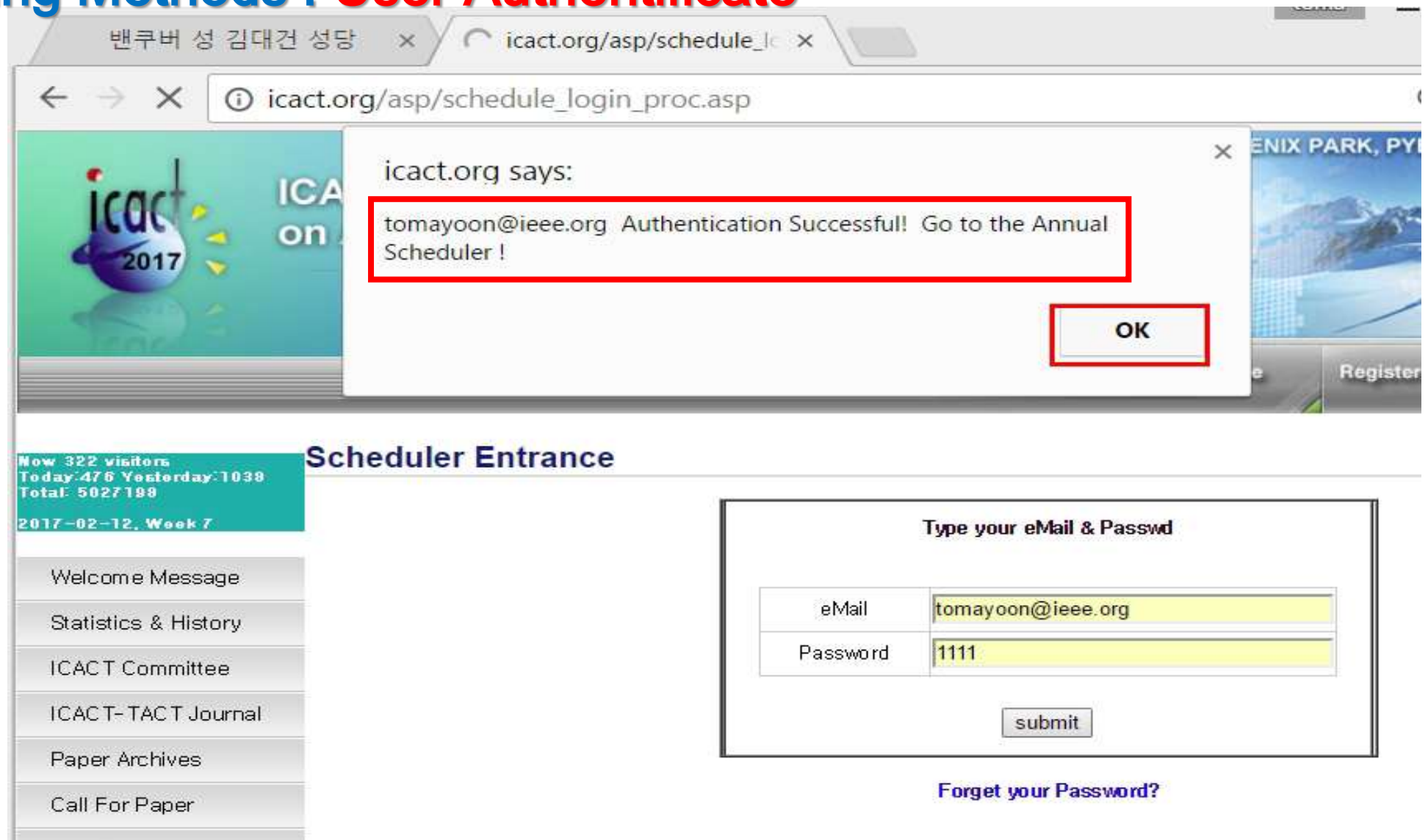
```
POST http://icact.org/asp/schedule_login_proc.asp HTTP/1.1
Host: icact.org
Proxy-Connection: keep-alive
Content-Length: 34
Cache-Control: max-age=0
Origin: http://icact.org
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0
.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,ko;q=0.8,en-US;q=0.6,en;q=0.4
Cookie: ASPSESSIONIDAQCCBTRS=NOOJLFHCDDOGAOBMCGIGMGAE; ASPSESSIONIDASCBDTQS=EFD
NIDEDEDAOFNPEBGHMAMJJ

eMail=tomayoon%40ieee.org&pwd=1111
```

Raw View | ☑ Trap request | ☐ Trap response | Continue | Drop

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
g/asp/schedule_login.asp	200	OK	2065ms



Cookie Programing Methods : User Authentificate



Web Service

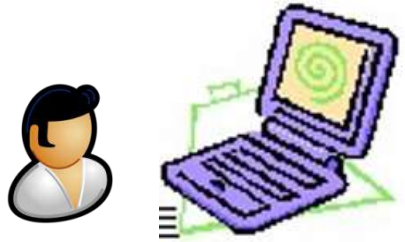
▶ Giri (tomayoon@ieee.org) Home Logout

Annual Schedule

ID_no(TCSnn, HOMnn, ORGnn, TPCnn, LOCnn) D-day(MM-DD)

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

Cyber Space Protocol – HTTP Response Status Code



Request(URL/URI)

Response(Status Code)

Web Browser

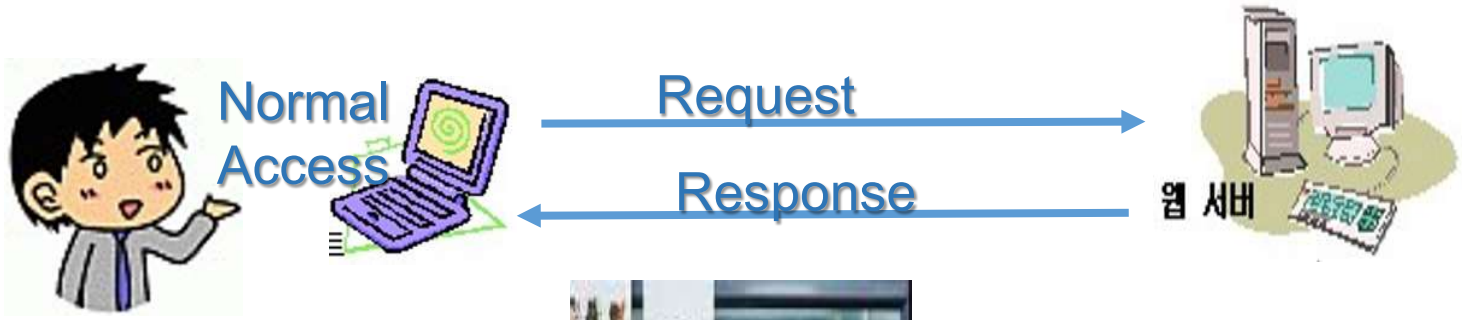
Web Server

- 200 : OK, Request Success
- 201 : File Created in Server
- 302 : Moved to Webpage (←Previous Webpage)
- 304 : Used Local Cache Info.
- 401 : Fail Authenticate
- 403 : Denied Access
- 404 : Not Exist Webpage
- 500 : Severe Error (DB Access Error ← Injection)

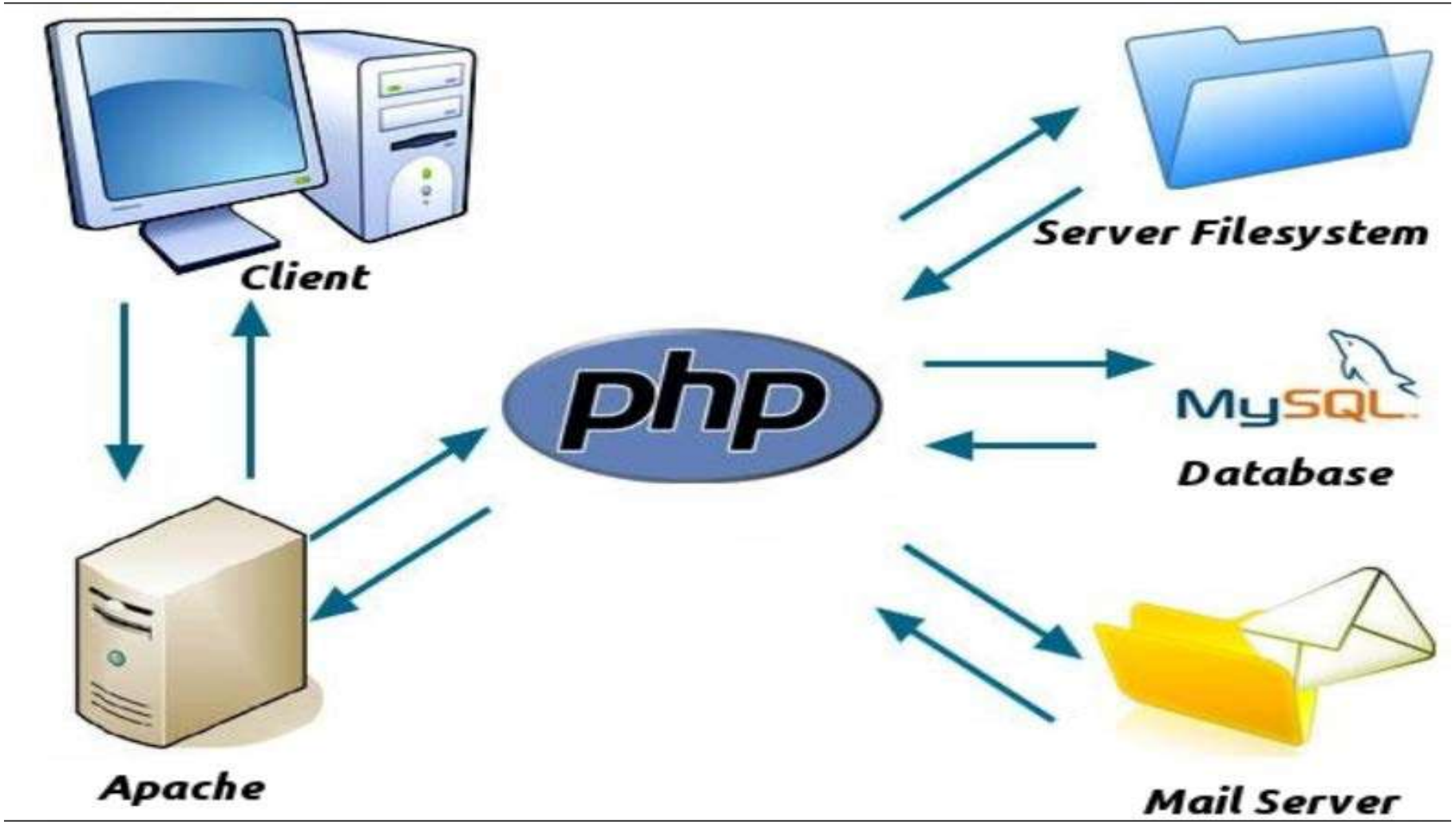
Web Log Analysis Scan

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...	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?!



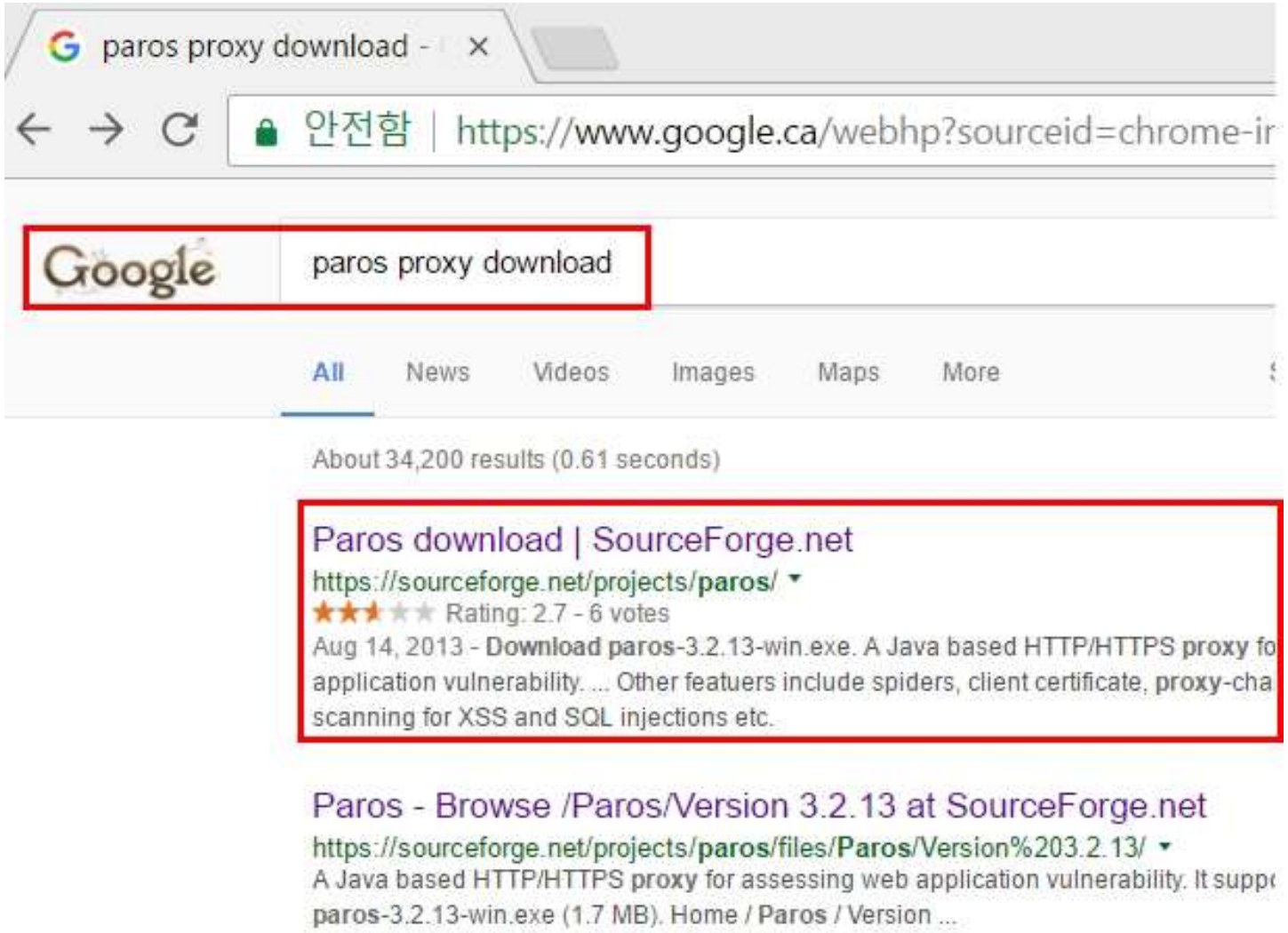
Paros – Open Source HTTP Intercept Tool!!

HTTP Intercept Tool - Paros!!

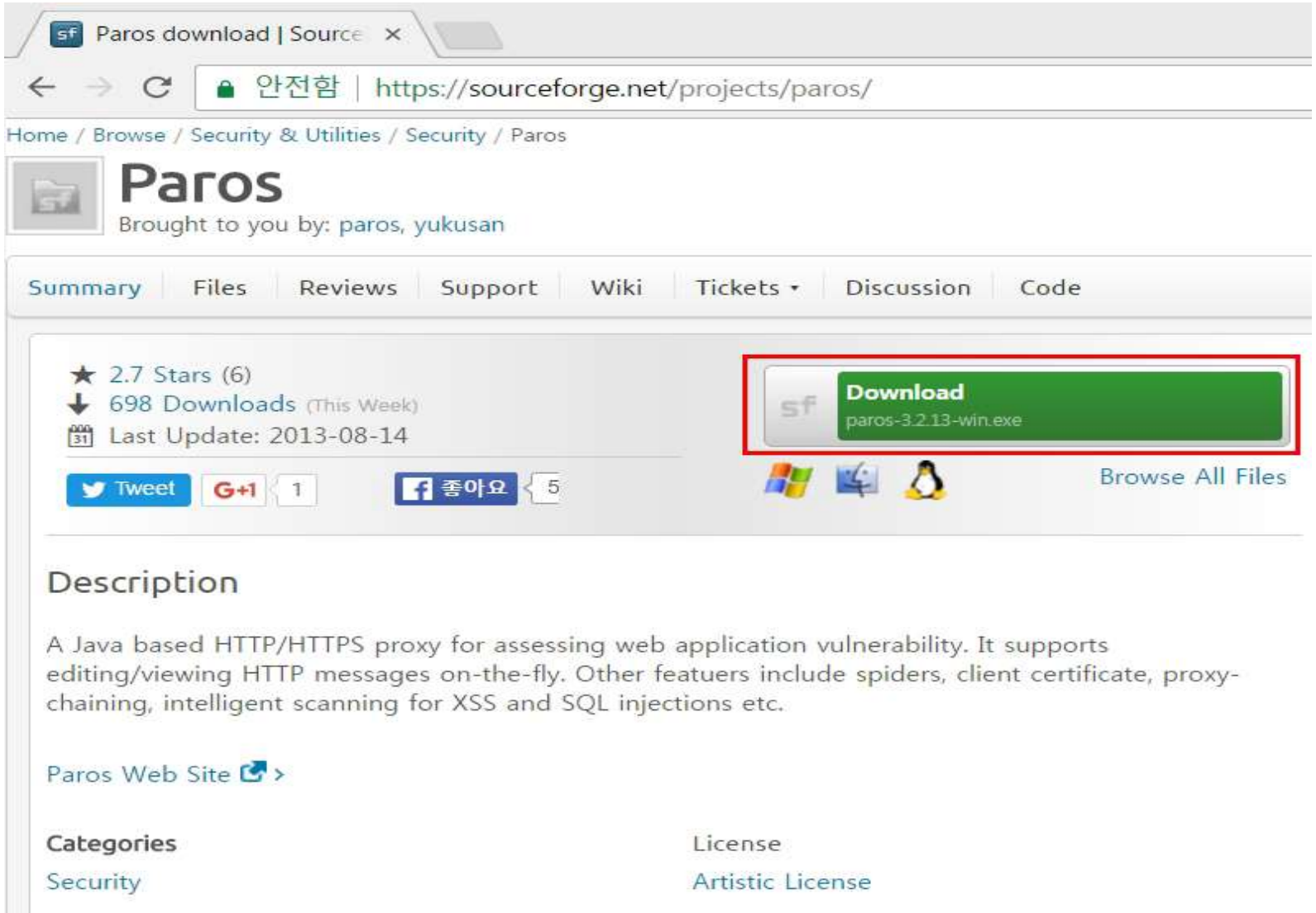
Paros Client Proxy Capability

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

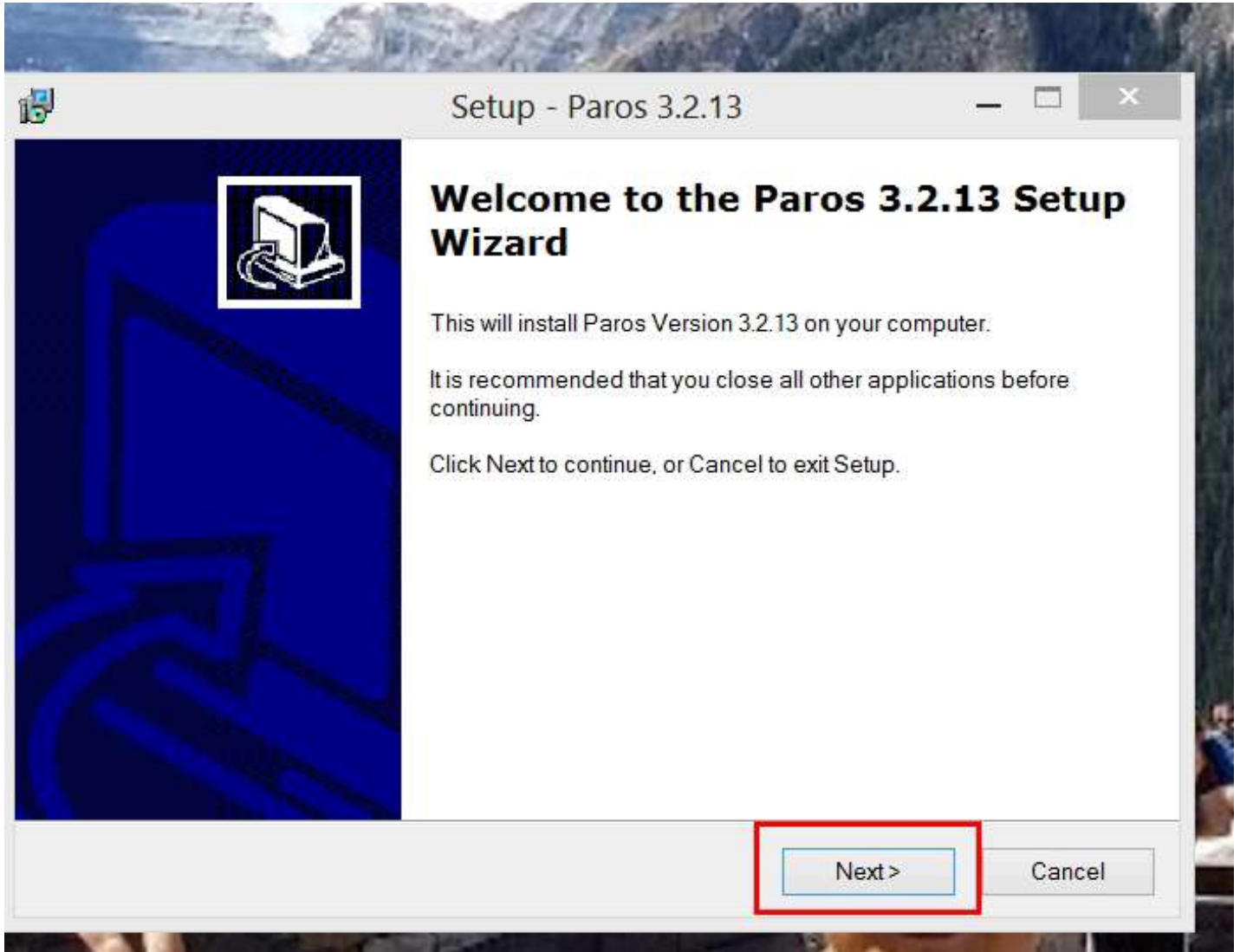
HTTP Intercept Tool – Paros Installation !!



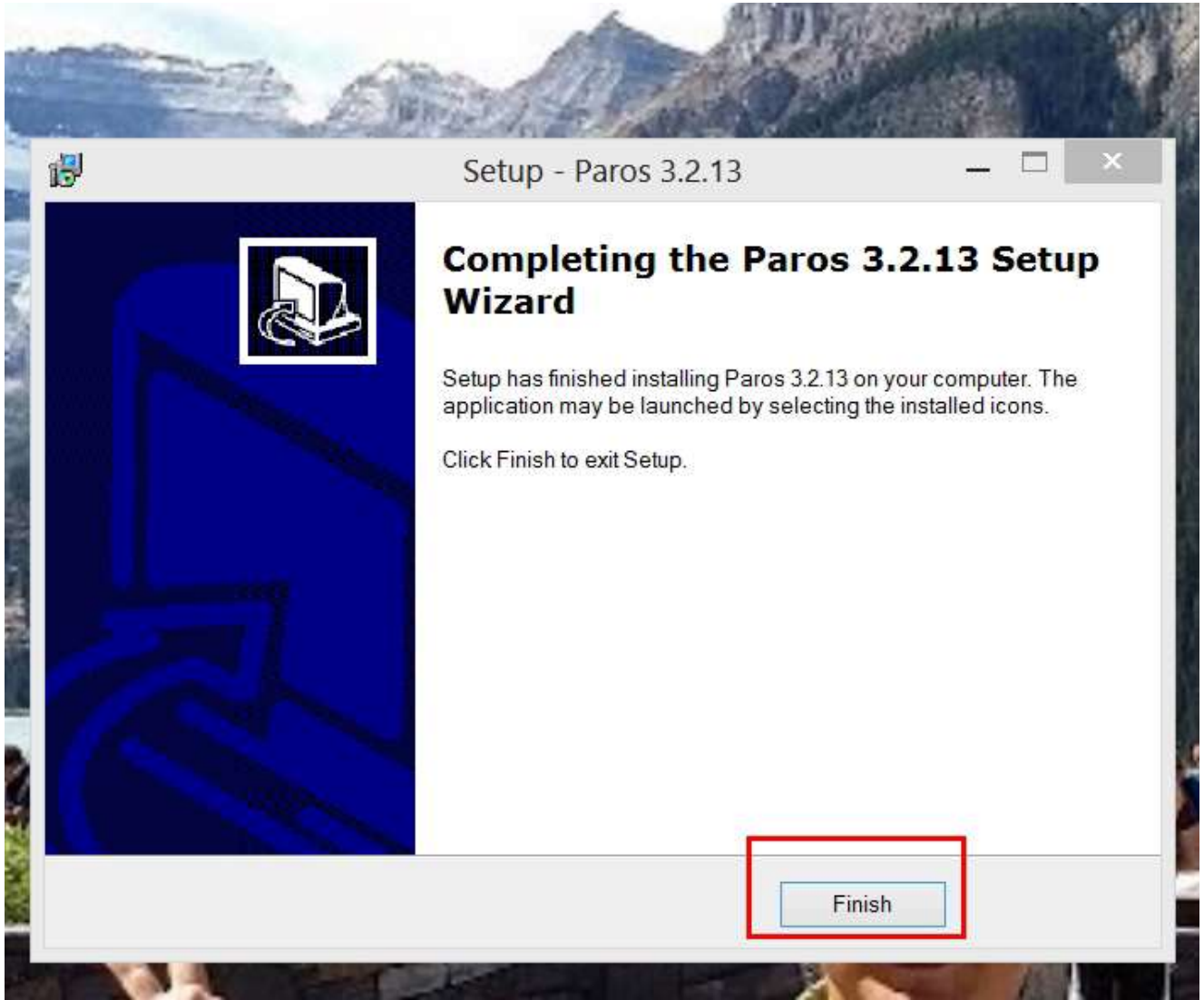
HTTP Intercept Tool – Paros Installation !!



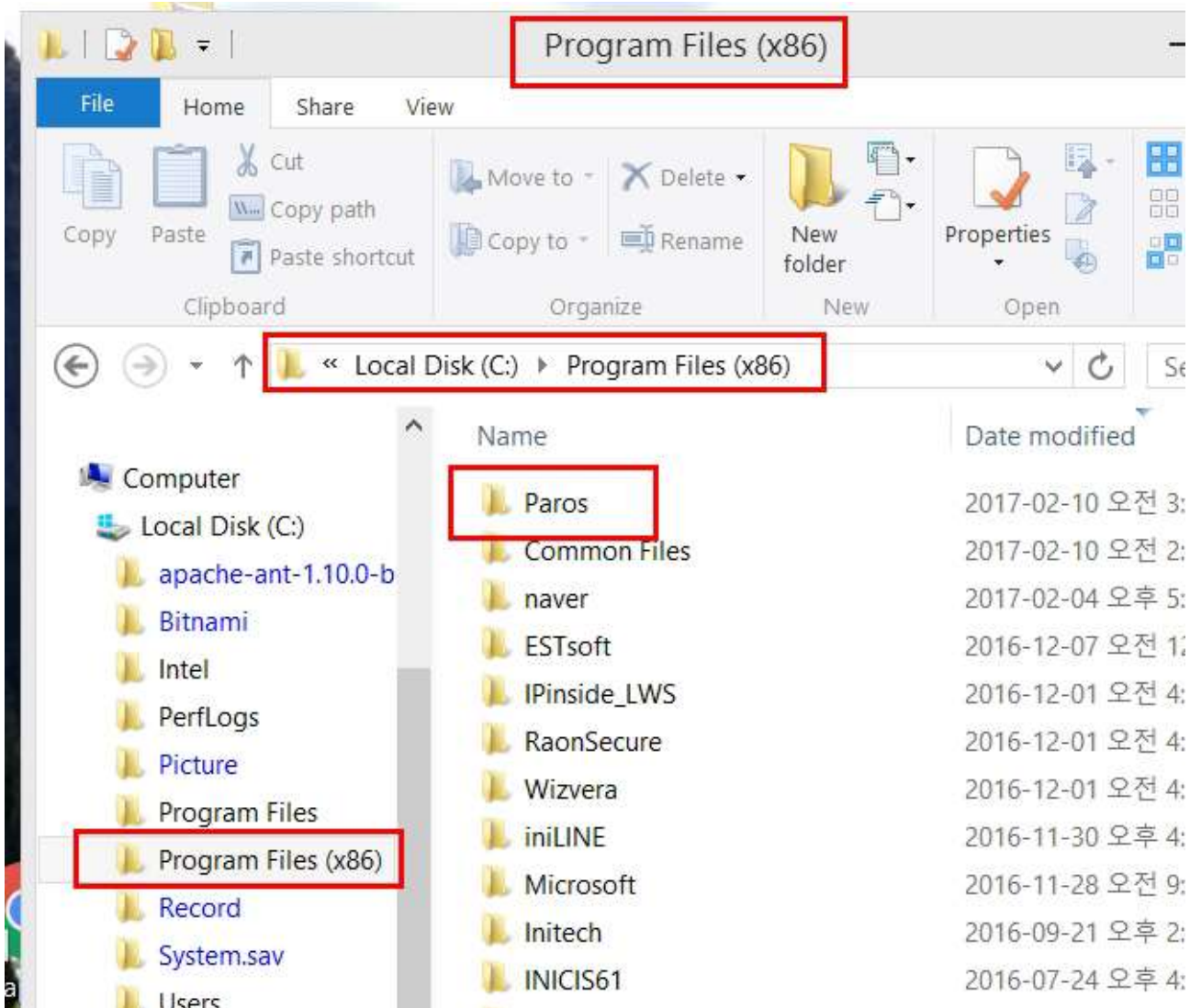
HTTP Intercept Tool – Paros Installation !!



HTTP Intercept Tool – Paros Installation !!



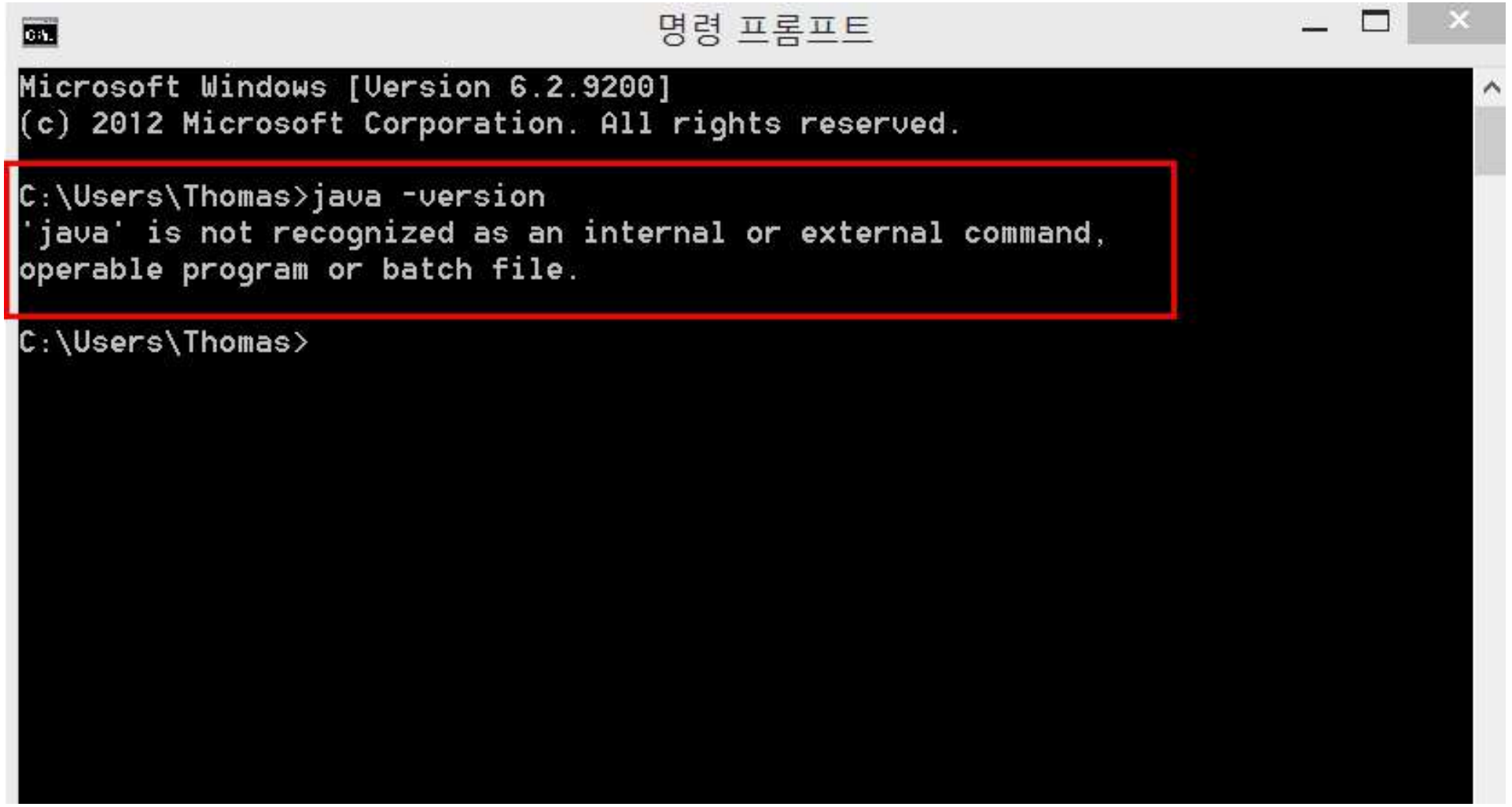
Paros Developed for x86 environment only



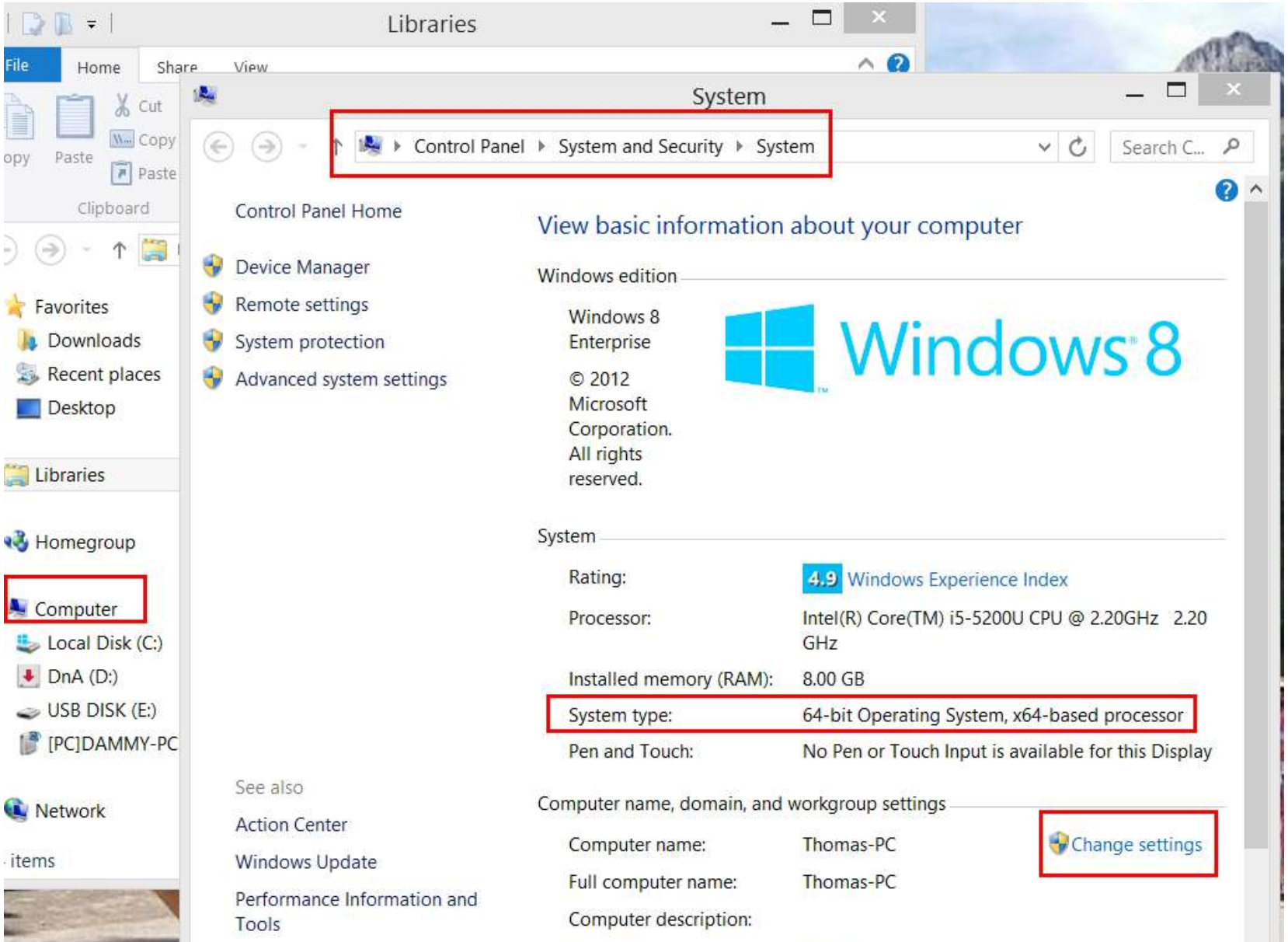
Paros Execution

Paros is Java Application

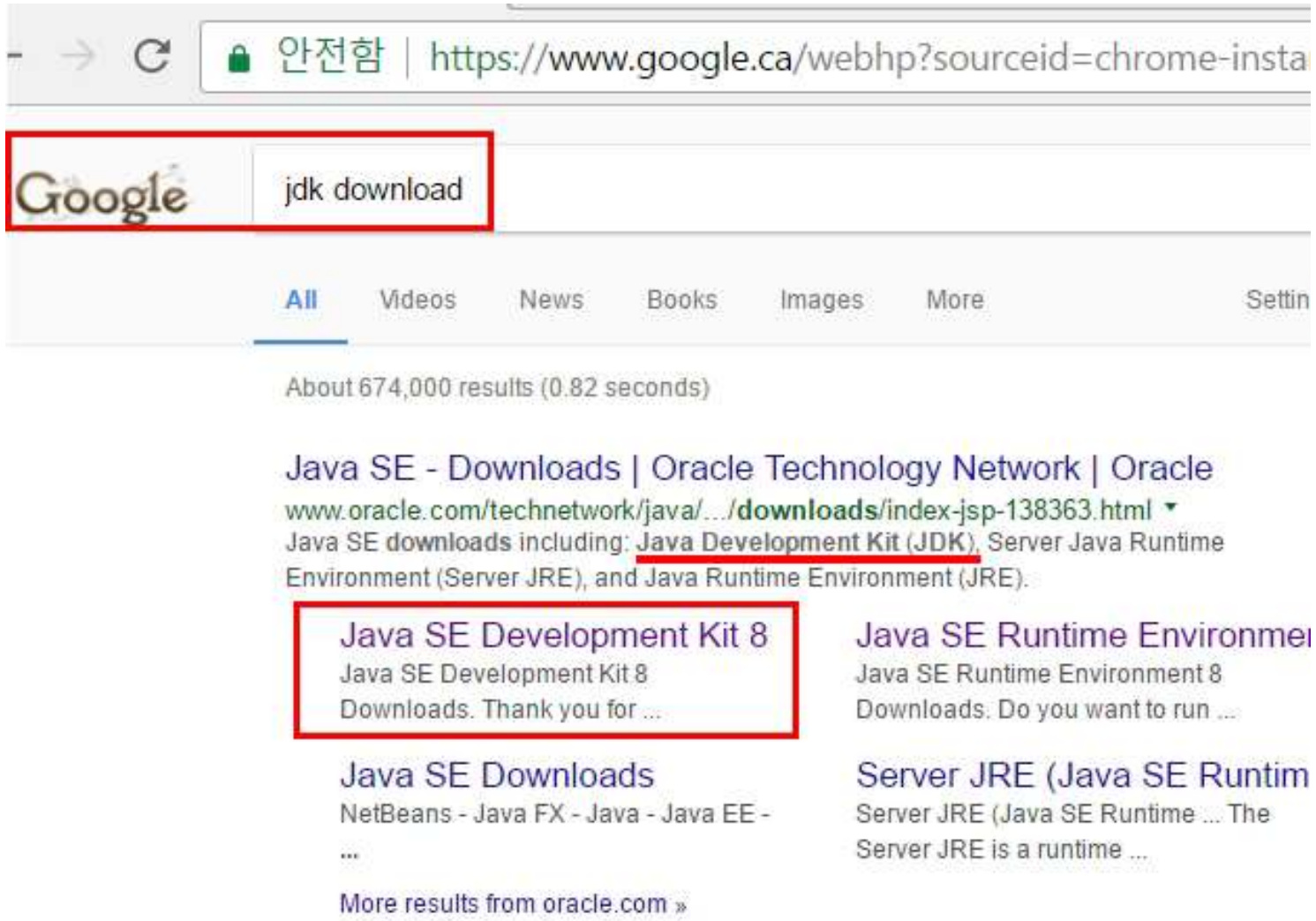
Paros needs JDK



JDK Installation !!



JDK Installation !!



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

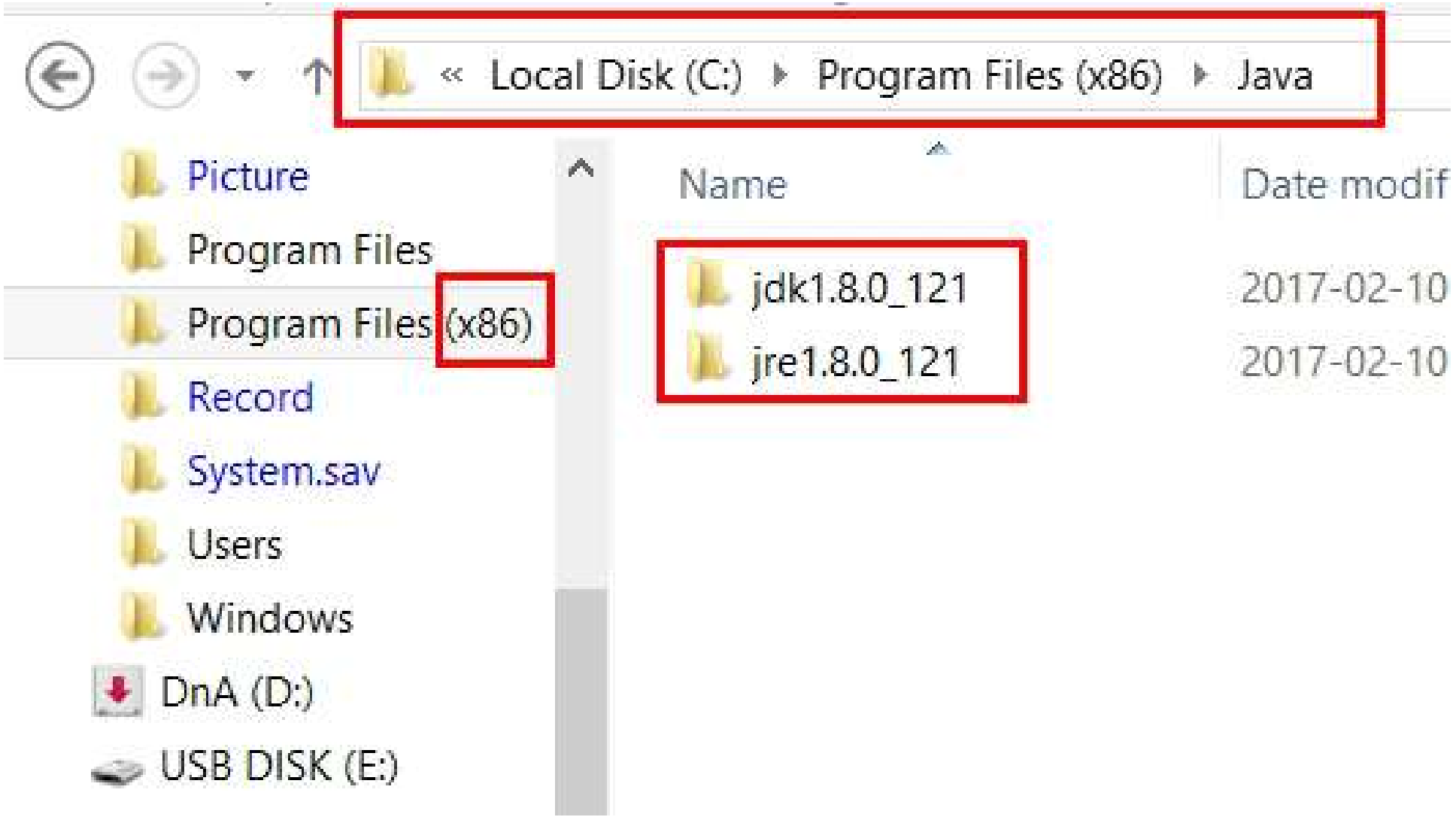
Product / File Description	File Size	Download
Linux ARM 32 Hard Float ABI	77.86 MB	jdk-8u121-linux-arm32-vfp-hflt.tar.gz
Linux ARM 64 Hard Float ABI	74.83 MB	jdk-8u121-linux-arm64-vfp-hflt.tar.gz
Linux x86	162.41 MB	jdk-8u121-linux-i586.rpm
Linux x86	177.13 MB	jdk-8u121-linux-i586.tar.gz
Linux x64	159.96 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
Windows x86	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

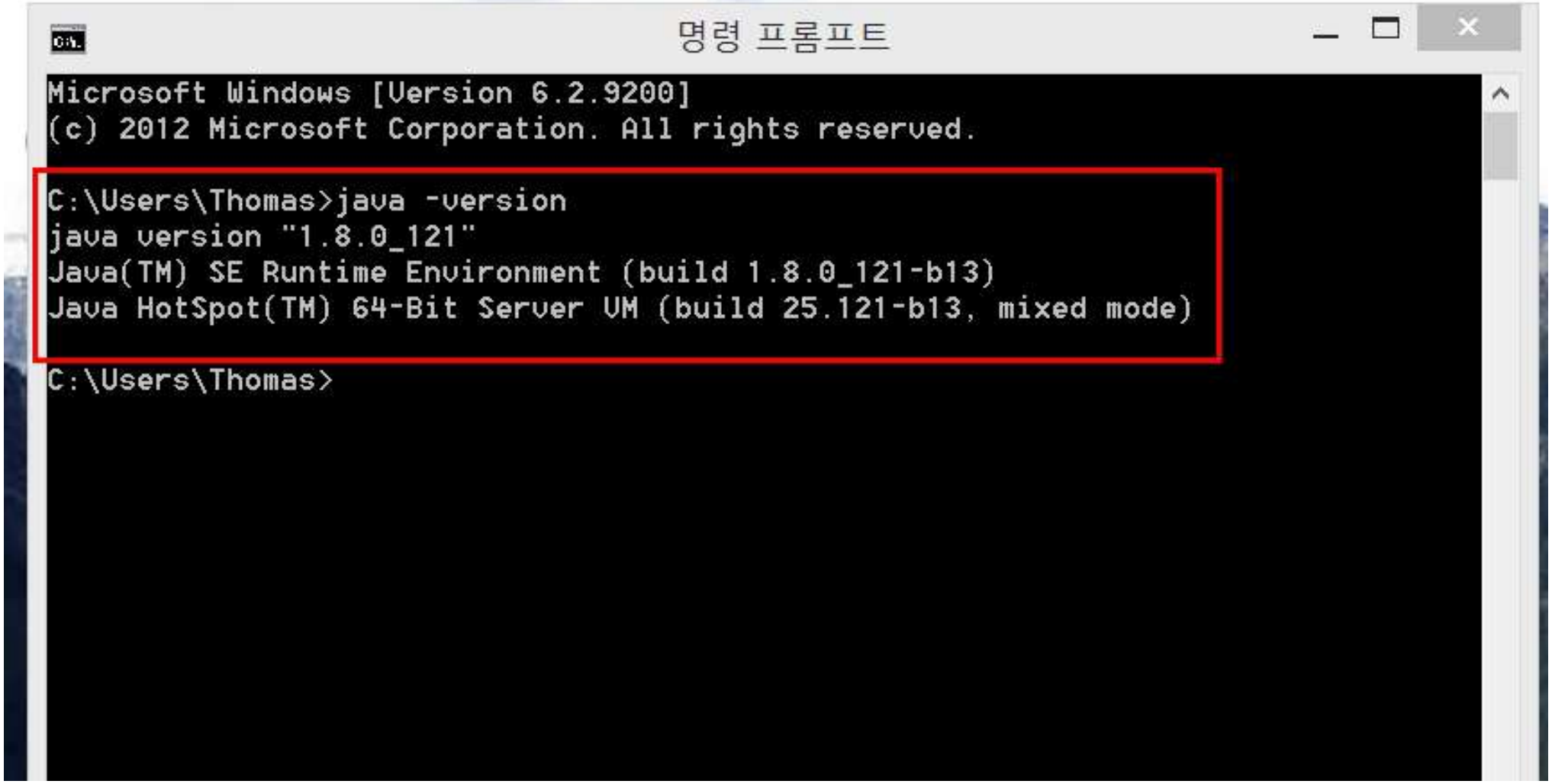
JDK Installation !!

JDK Installation Completed !!

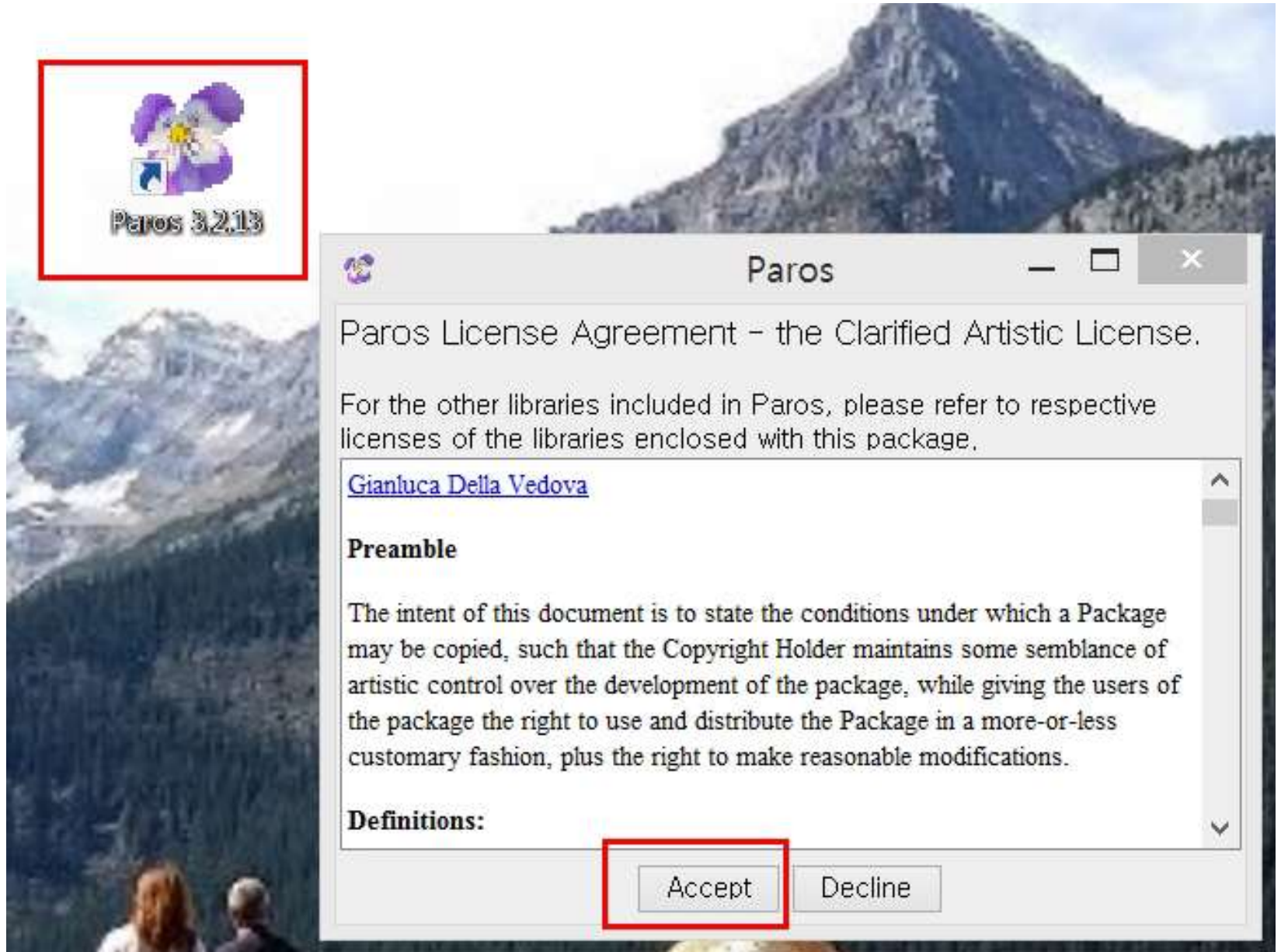
JDK Installation x86 - Confirm !!



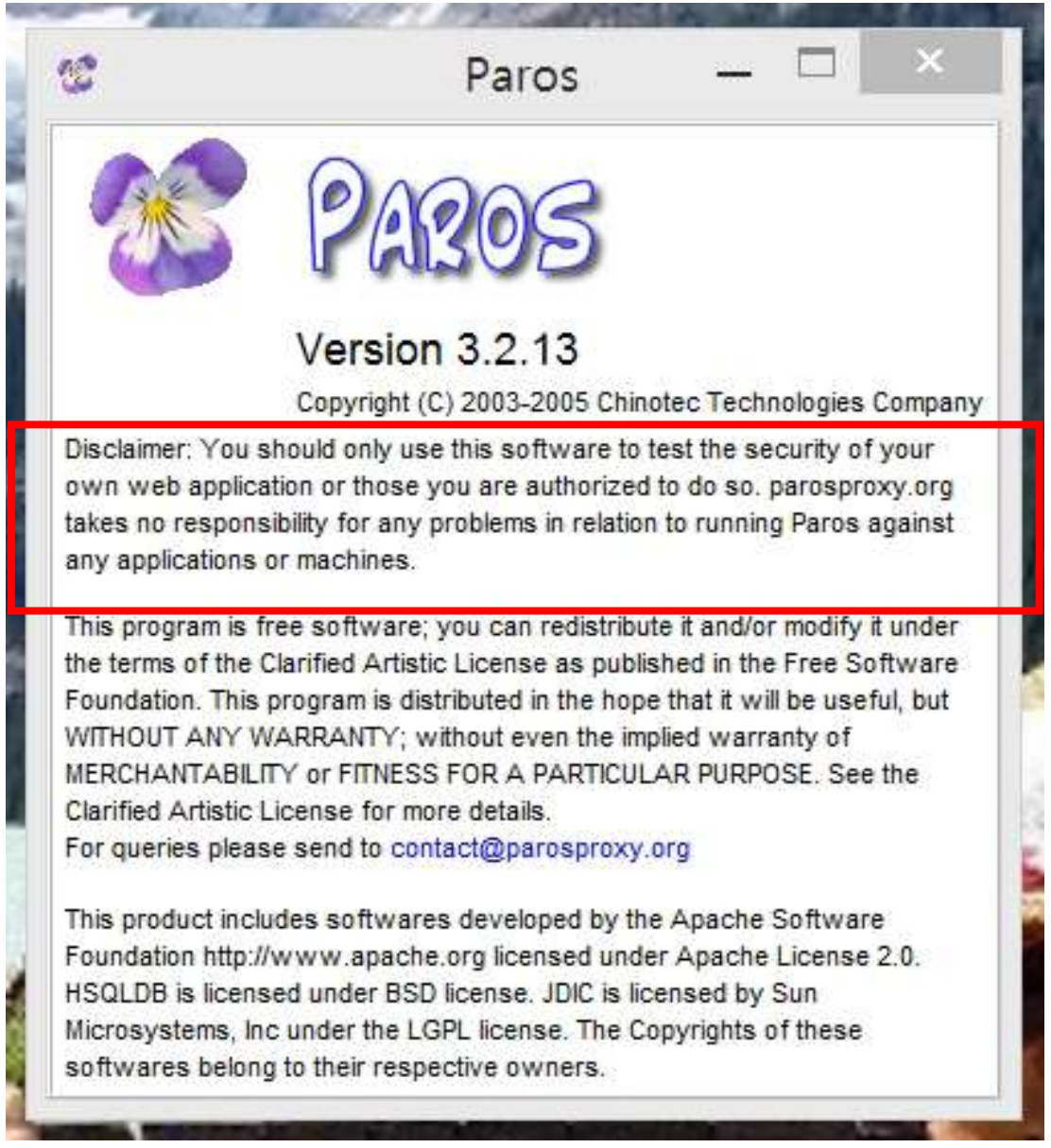
JDK Installation - Confirm !!



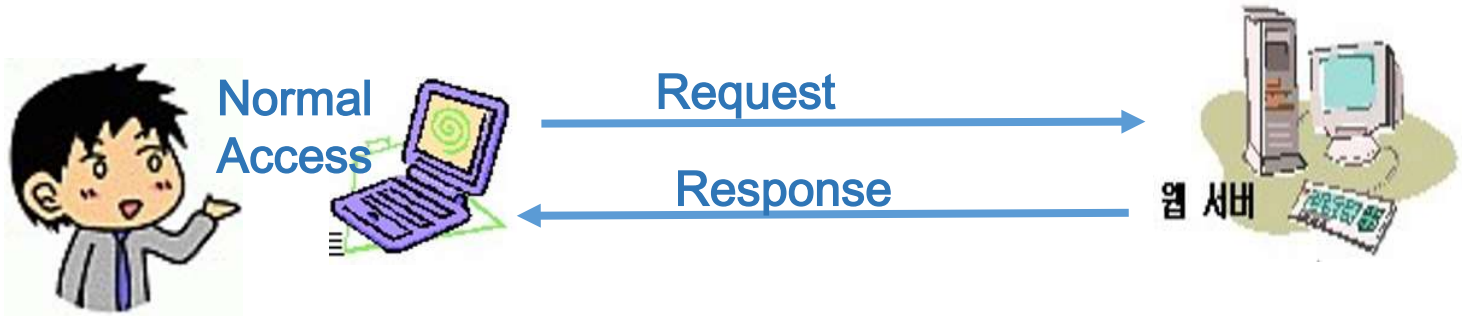
PAROS Execution

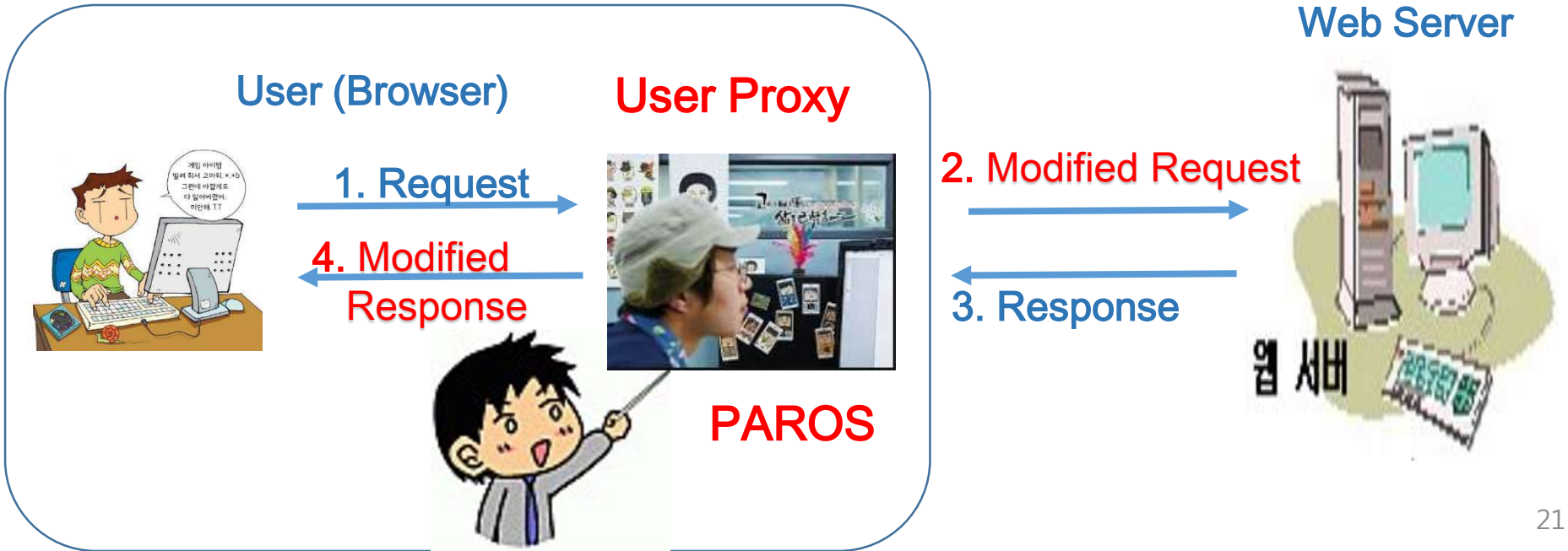


PAROS Execution



HTTP Intercept – PAROS Ready to Use!





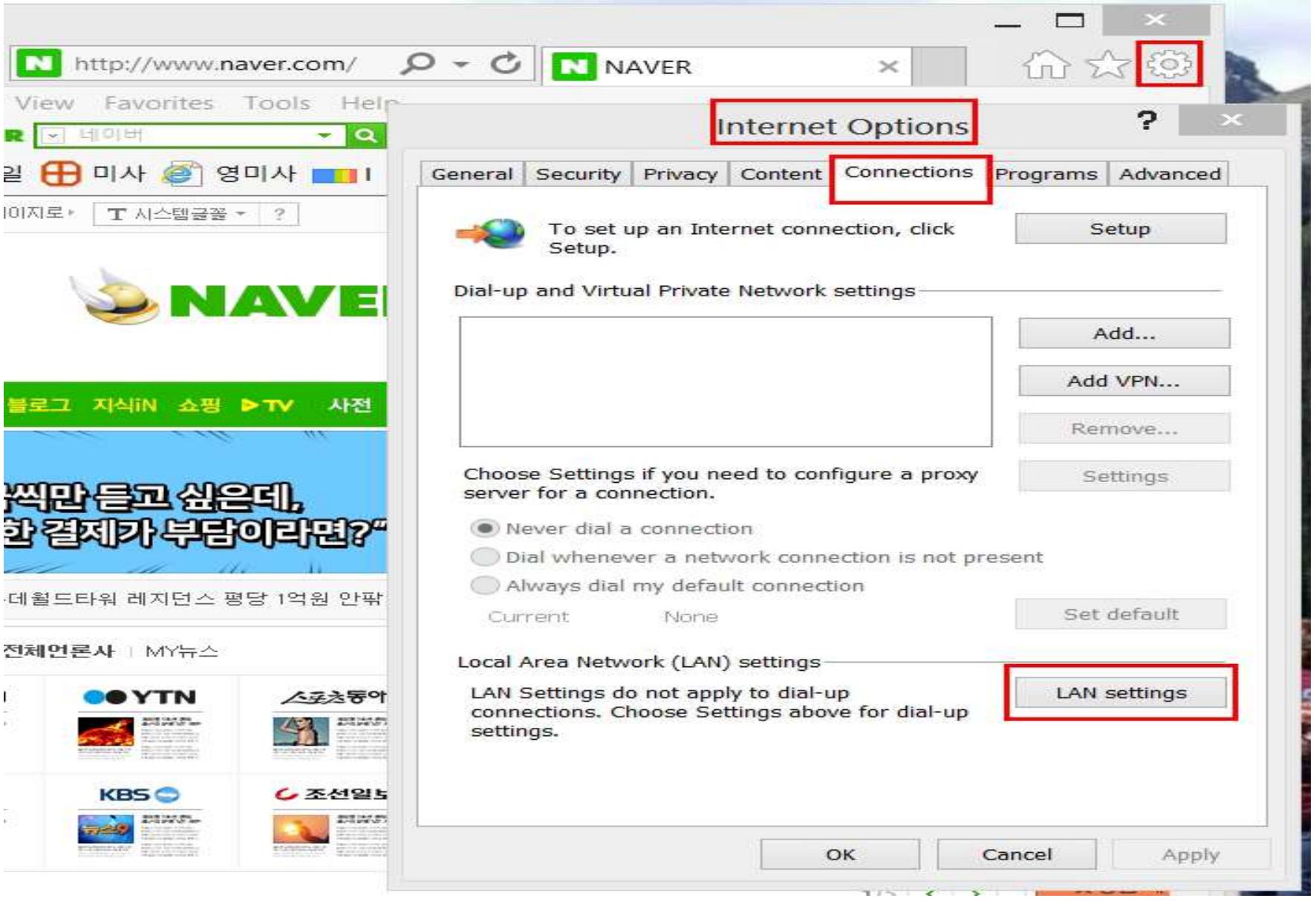
Cyber Space Hacking Tool – Paros

○ 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

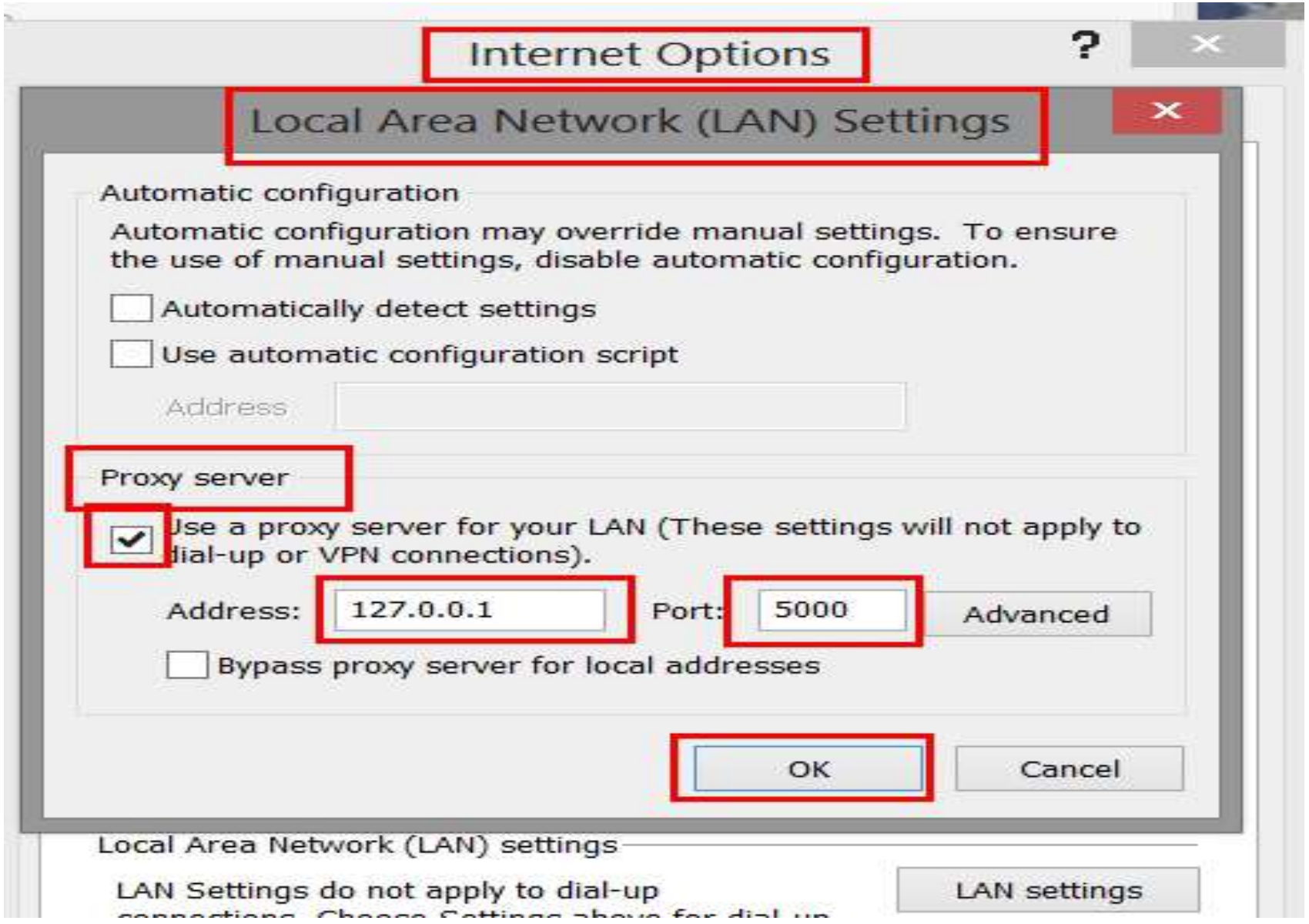
Proxy Server Setting

IE Browser

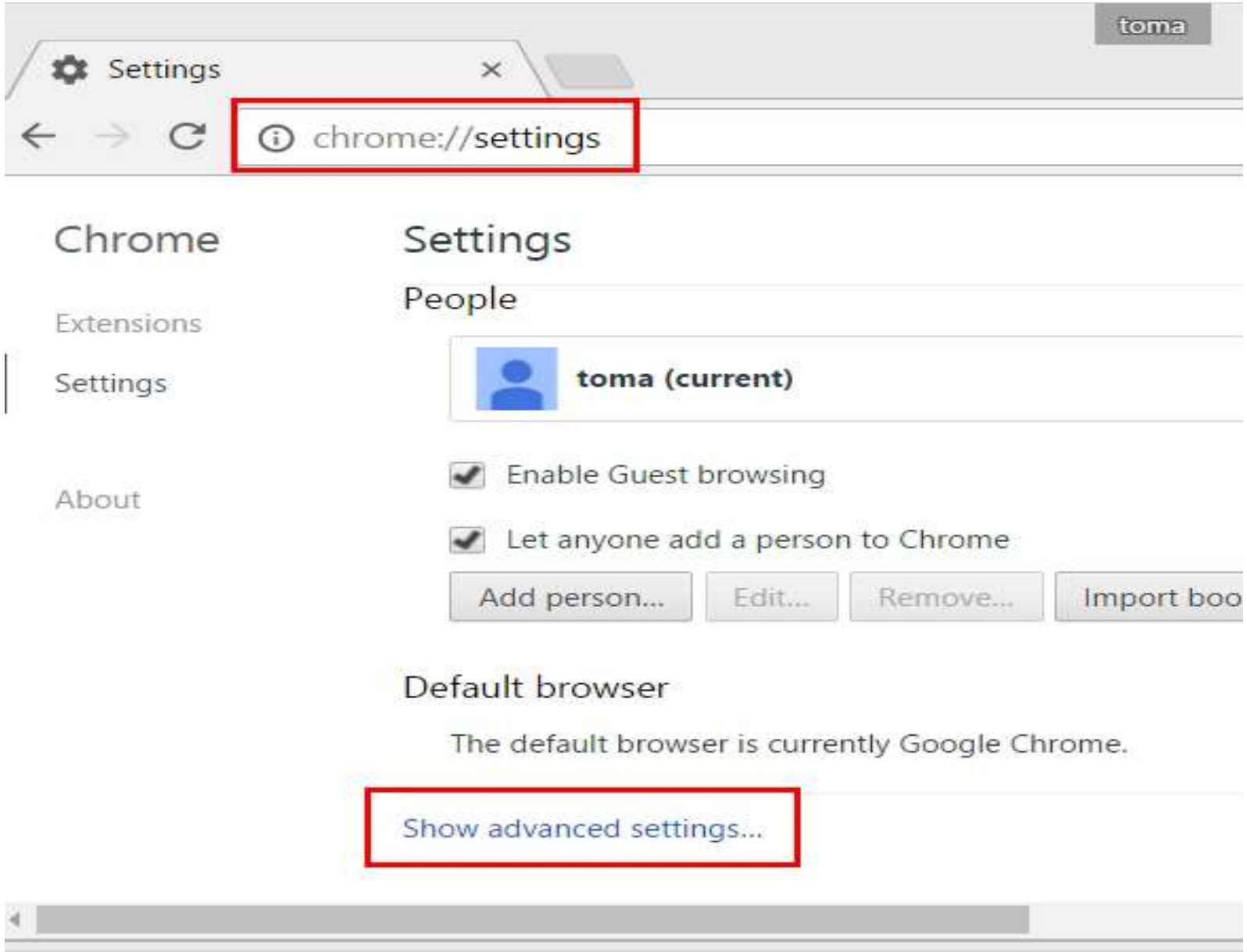


Proxy Server Setting

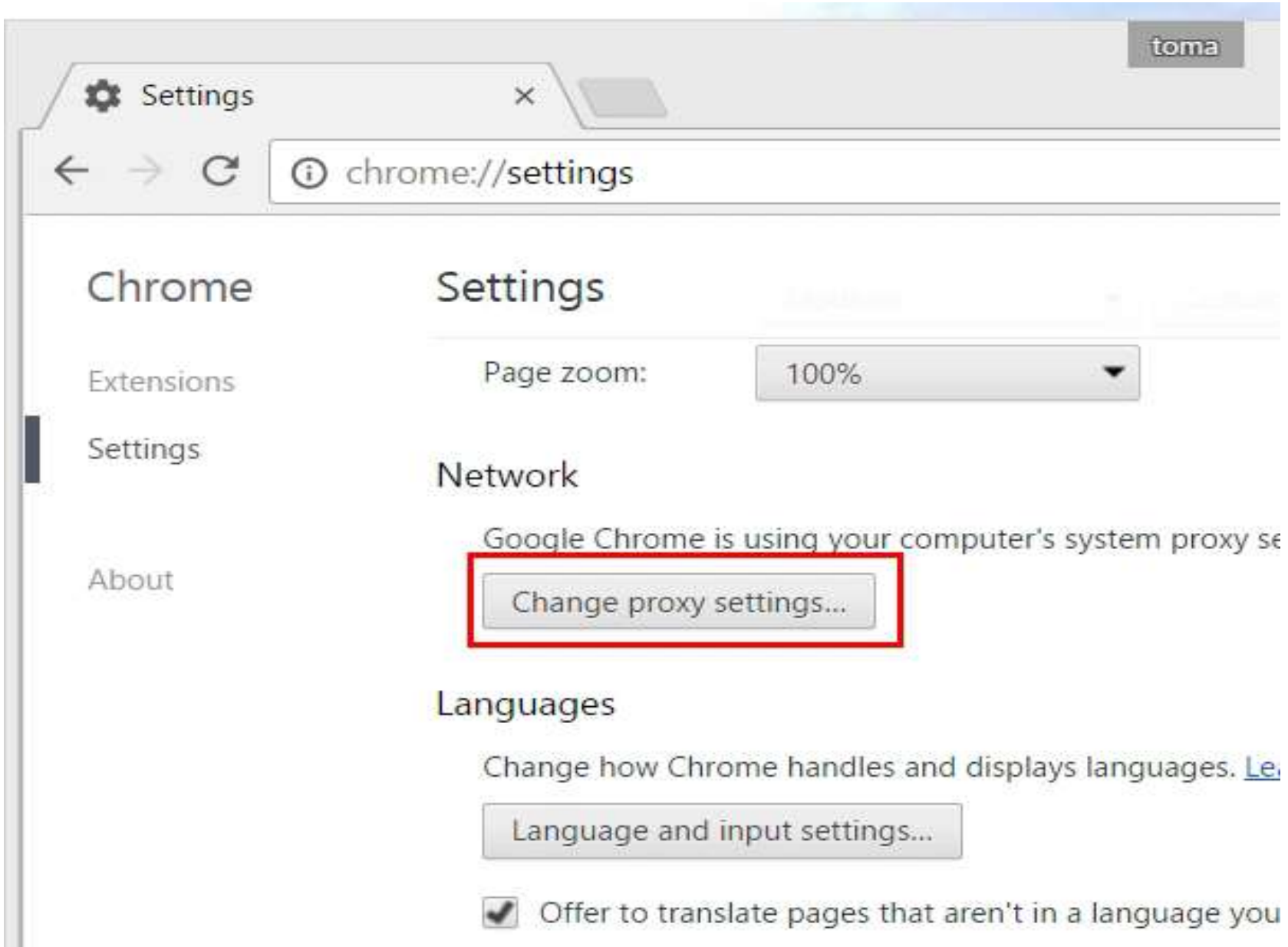
IE Browser



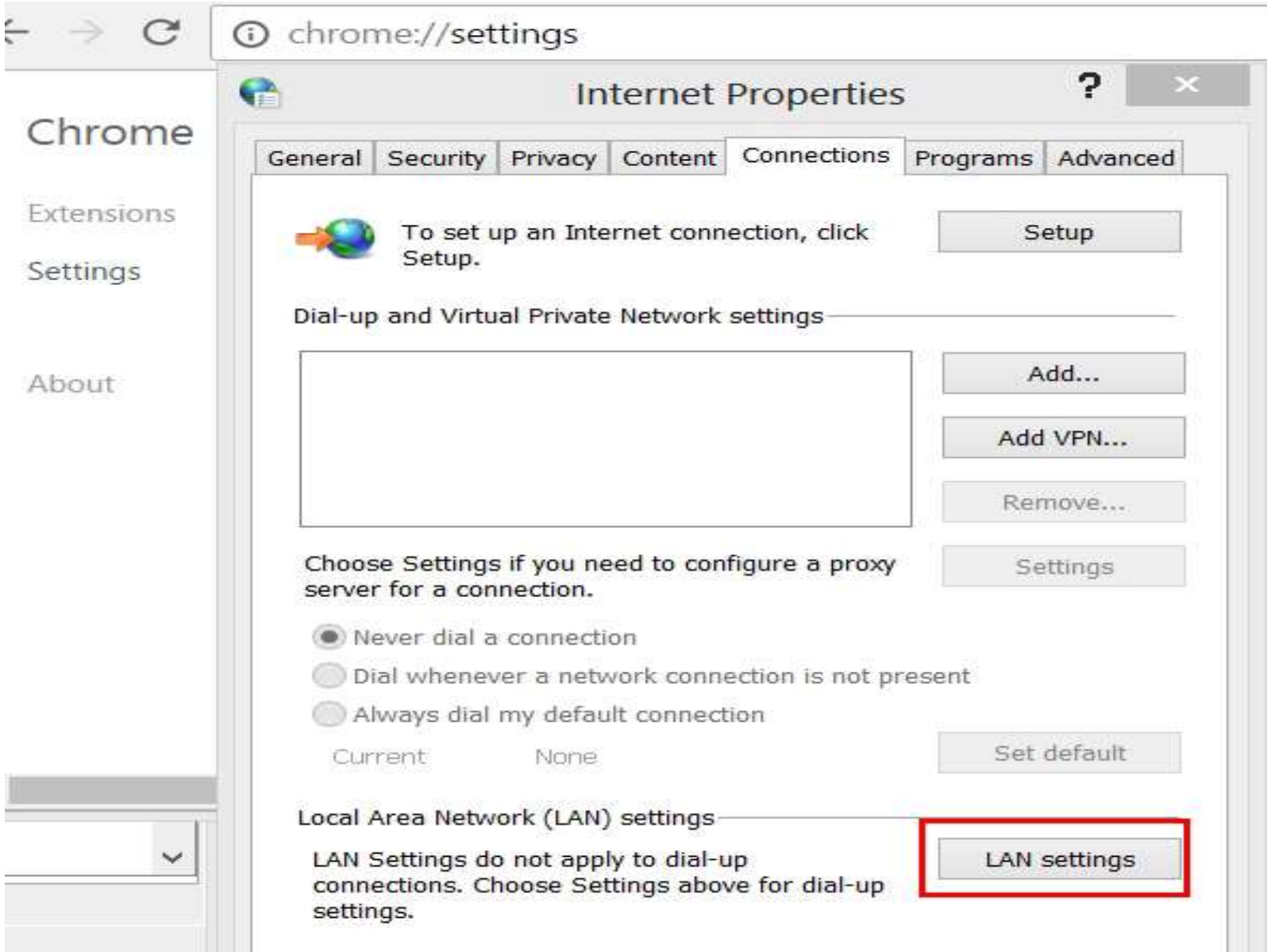
Proxy Server Setting
Chrome Browser



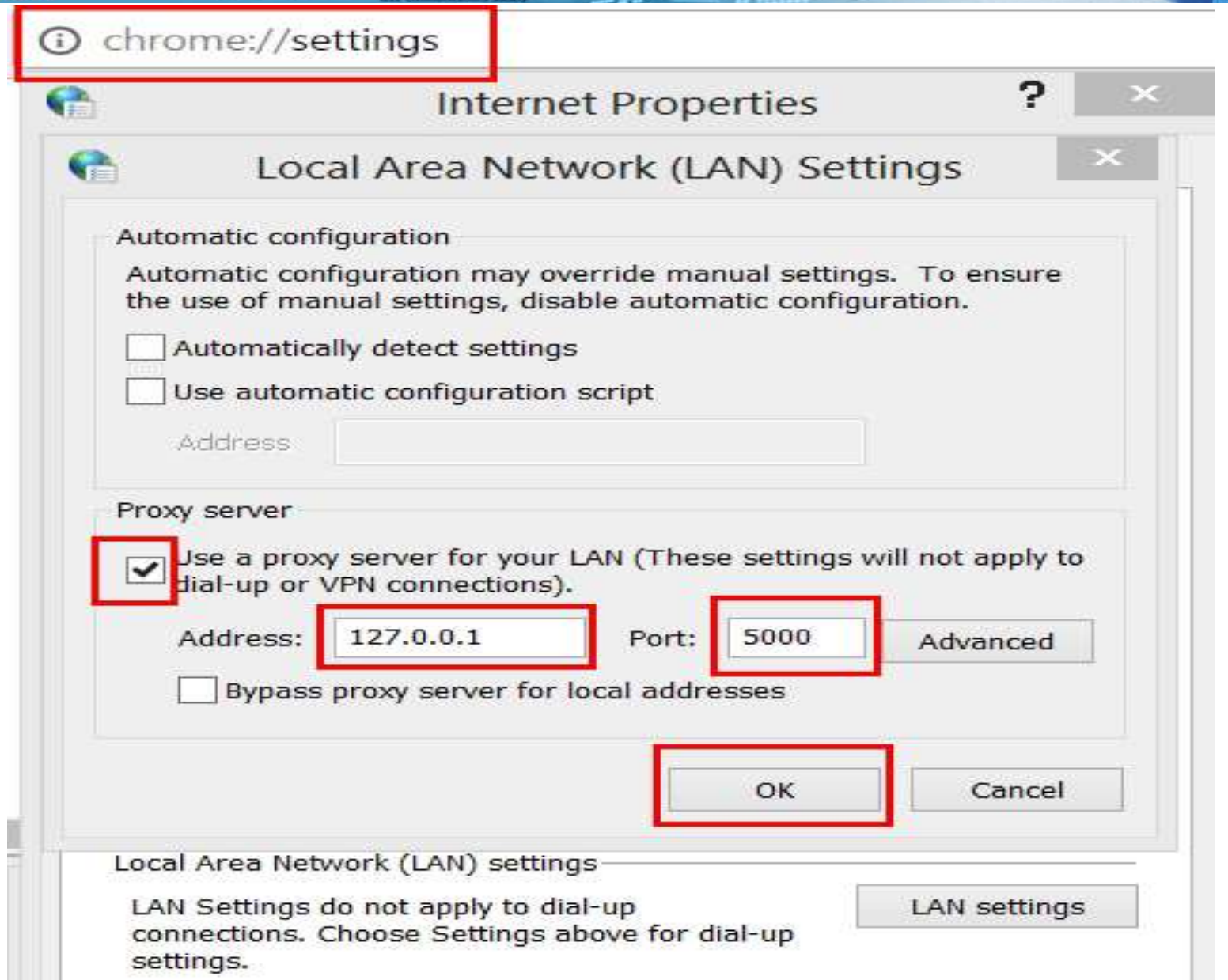
Proxy Server Setting
Chrome Browser



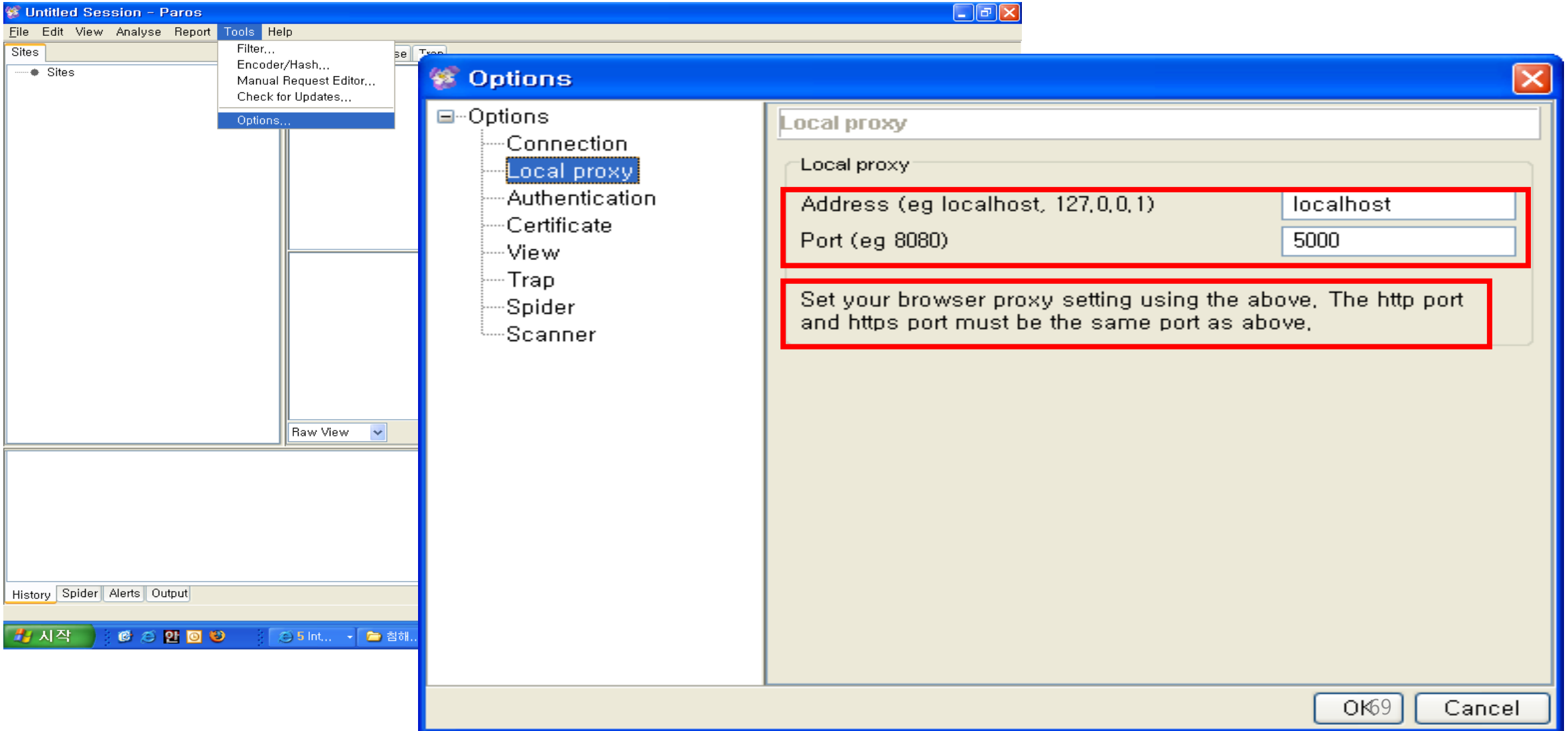
Proxy Server Setting
Chrome Browser



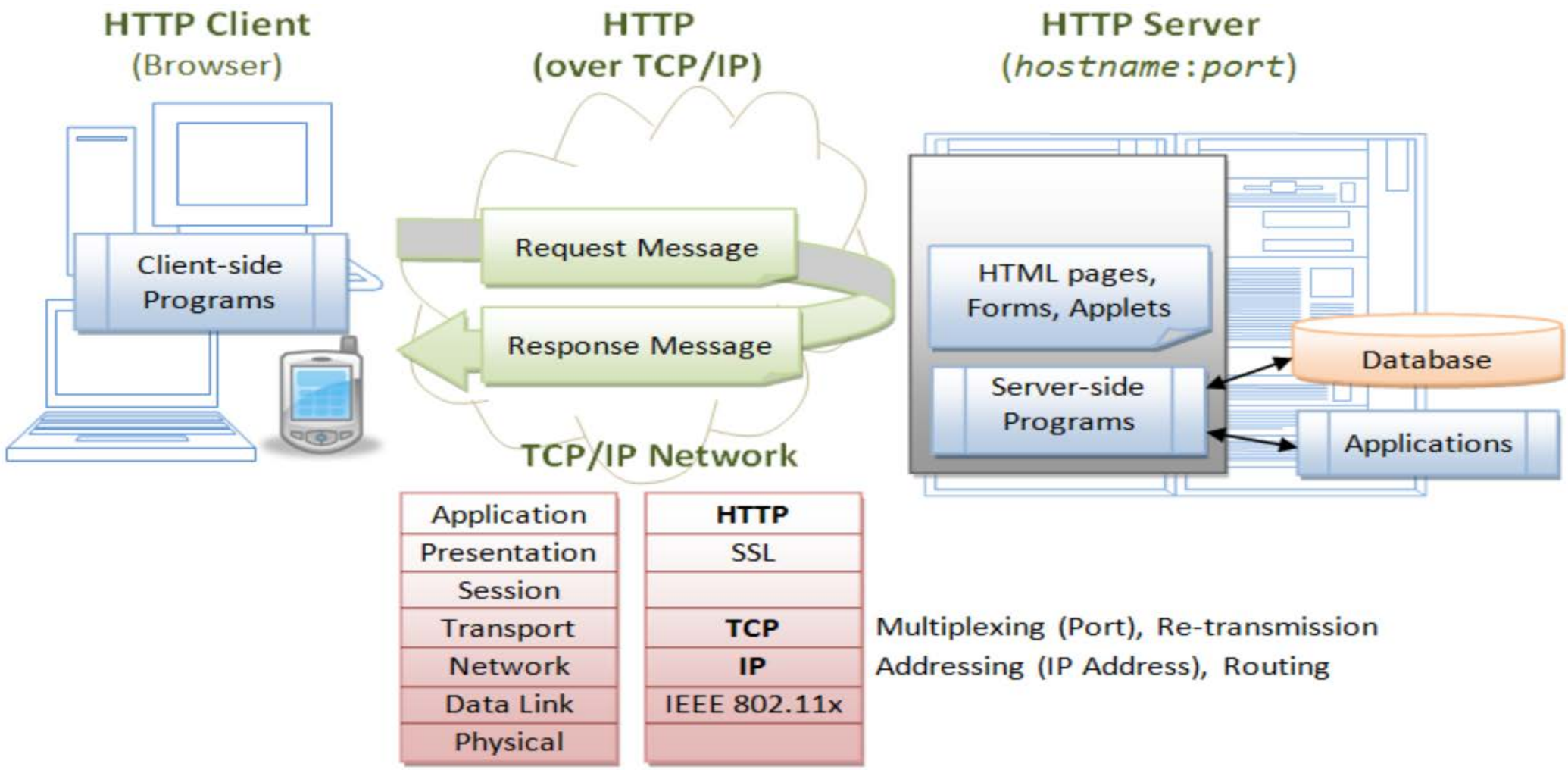
Proxy Server Setting
Chrome Browser



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



Web Port Number → Jump to Pertinent Service Program

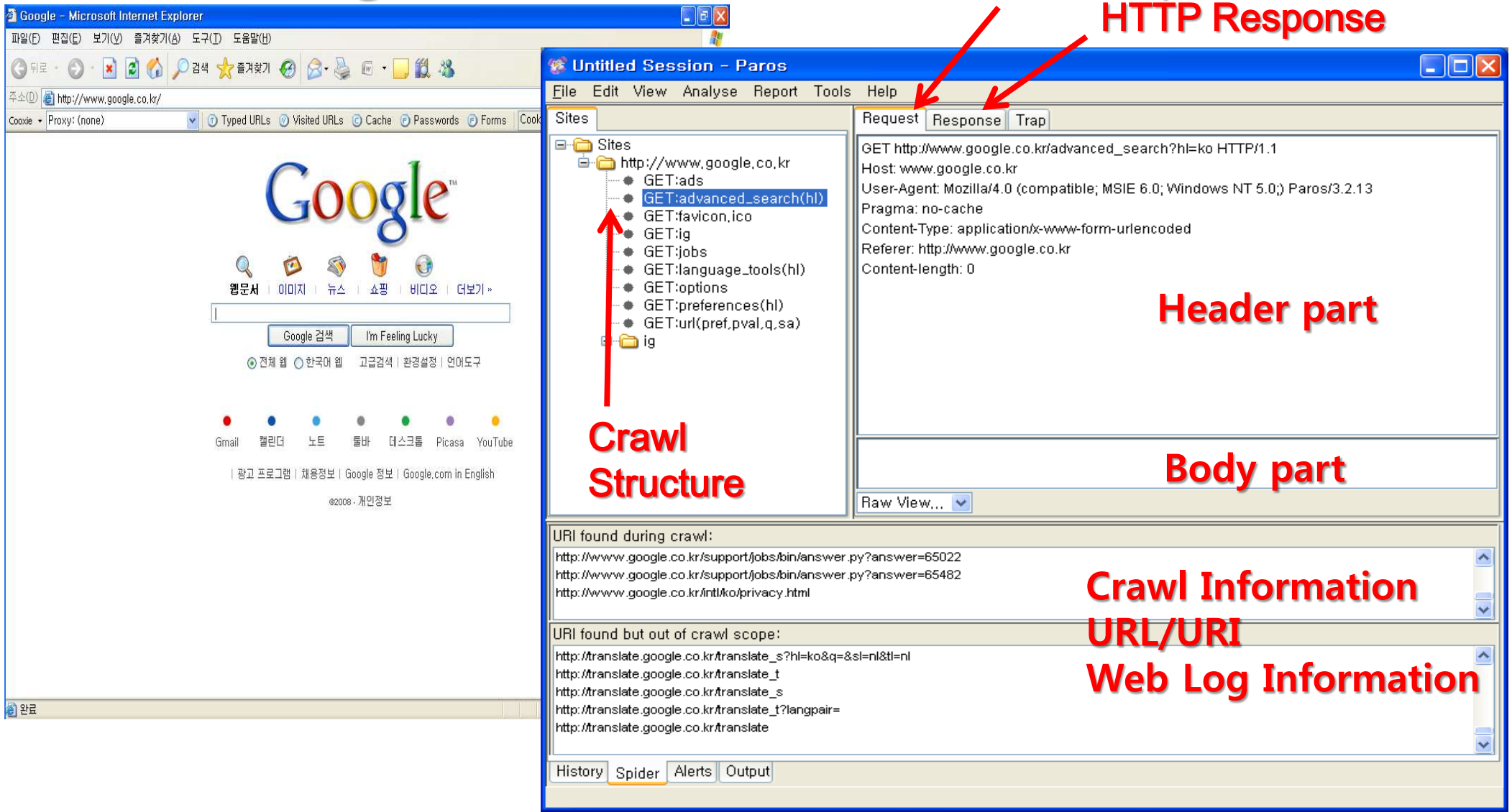


Web Port Number(16bits-64k) → Assigned Service Handler

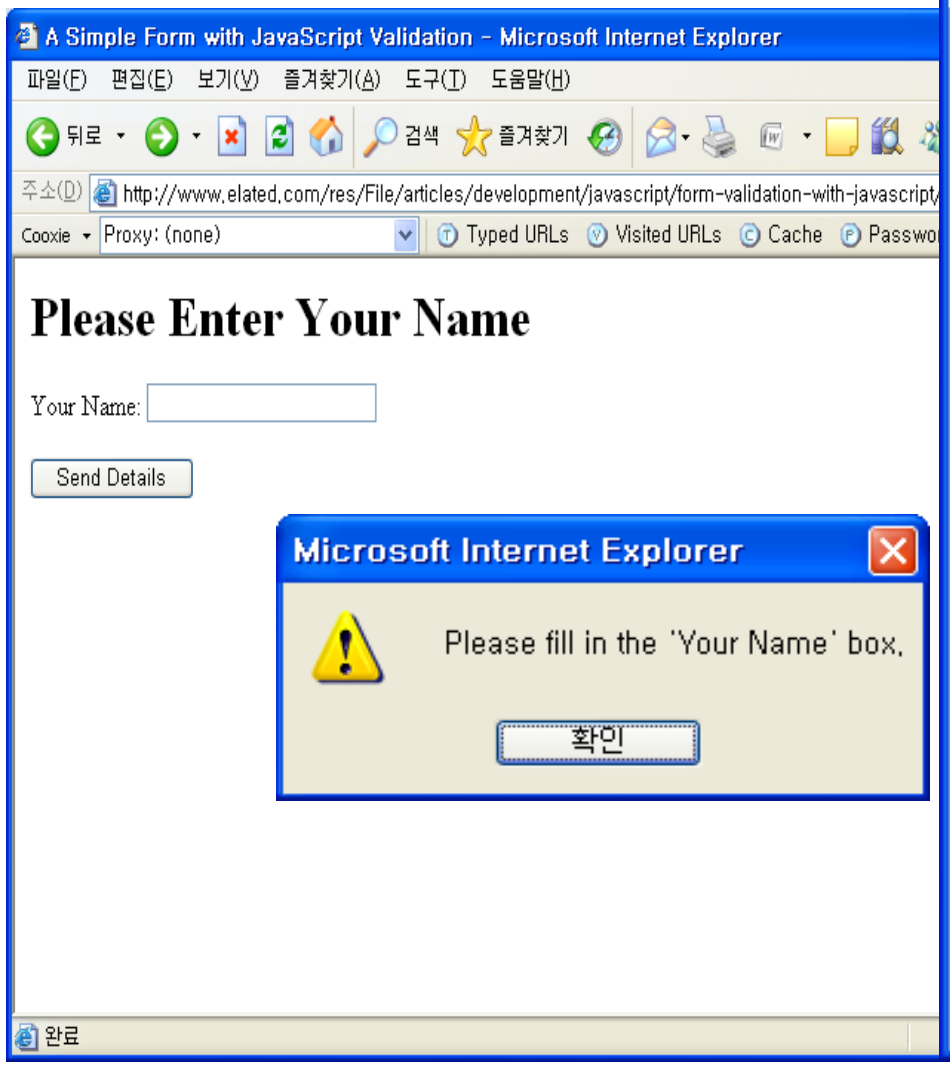
IANA: Internet Assigned Numbers Authority

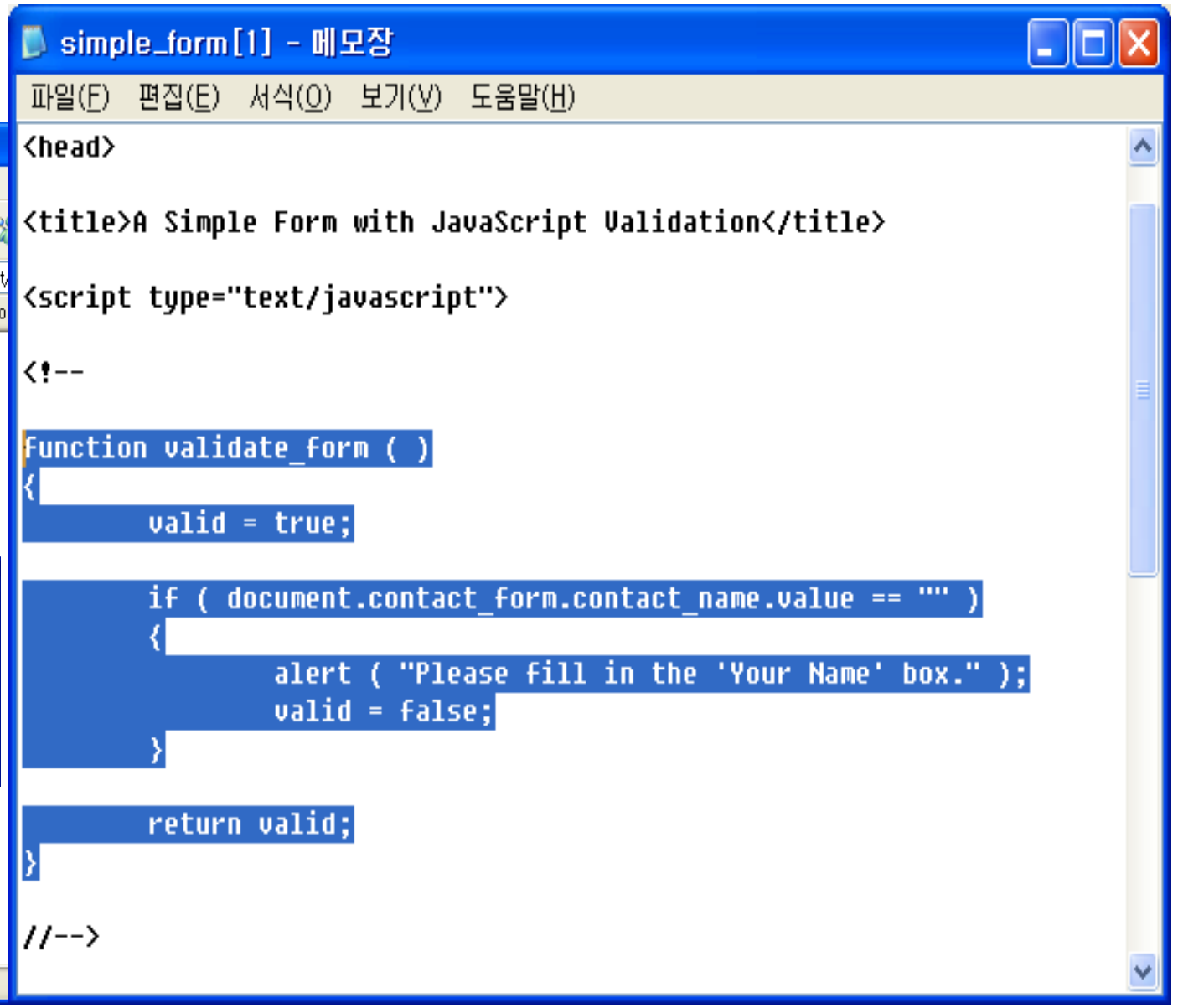
Label on Column	Service Name	UDP and TCP Port Numbers Included
DNS	Domain Name Service – UDP	UDP 53
DNS TCP	Domain Name Service – TCP	TCP 53
HTTP	Web	TCP 80
HTTPS	Secure Web (SSL)	TCP 443
SMTP	Simple Mail Transport	TCP 25
POP	Post Office Protocol	TCP 109, 110
SNMP	Simple Network Management	TCP 161,162 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

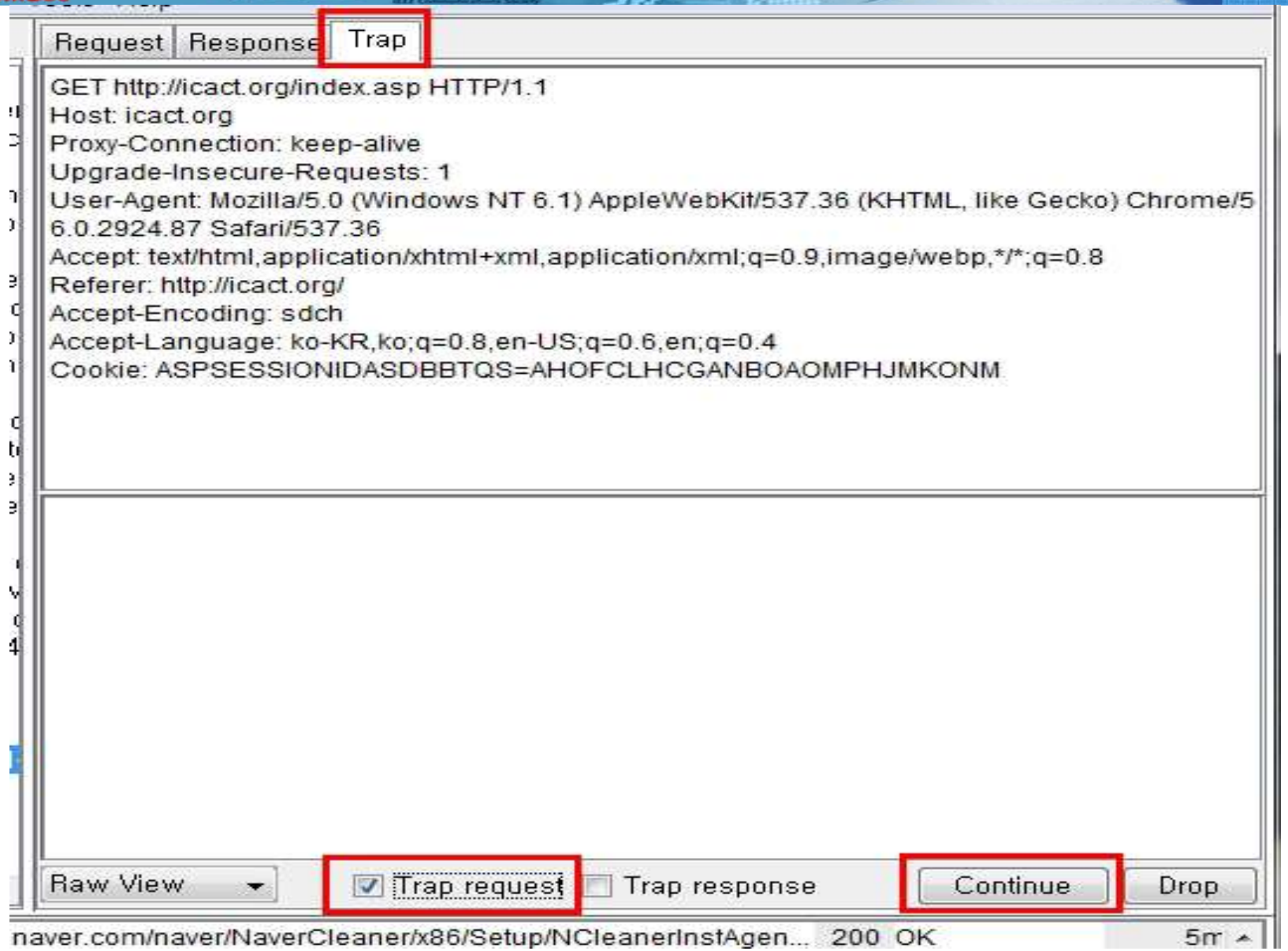


Paros modify HTTP Data

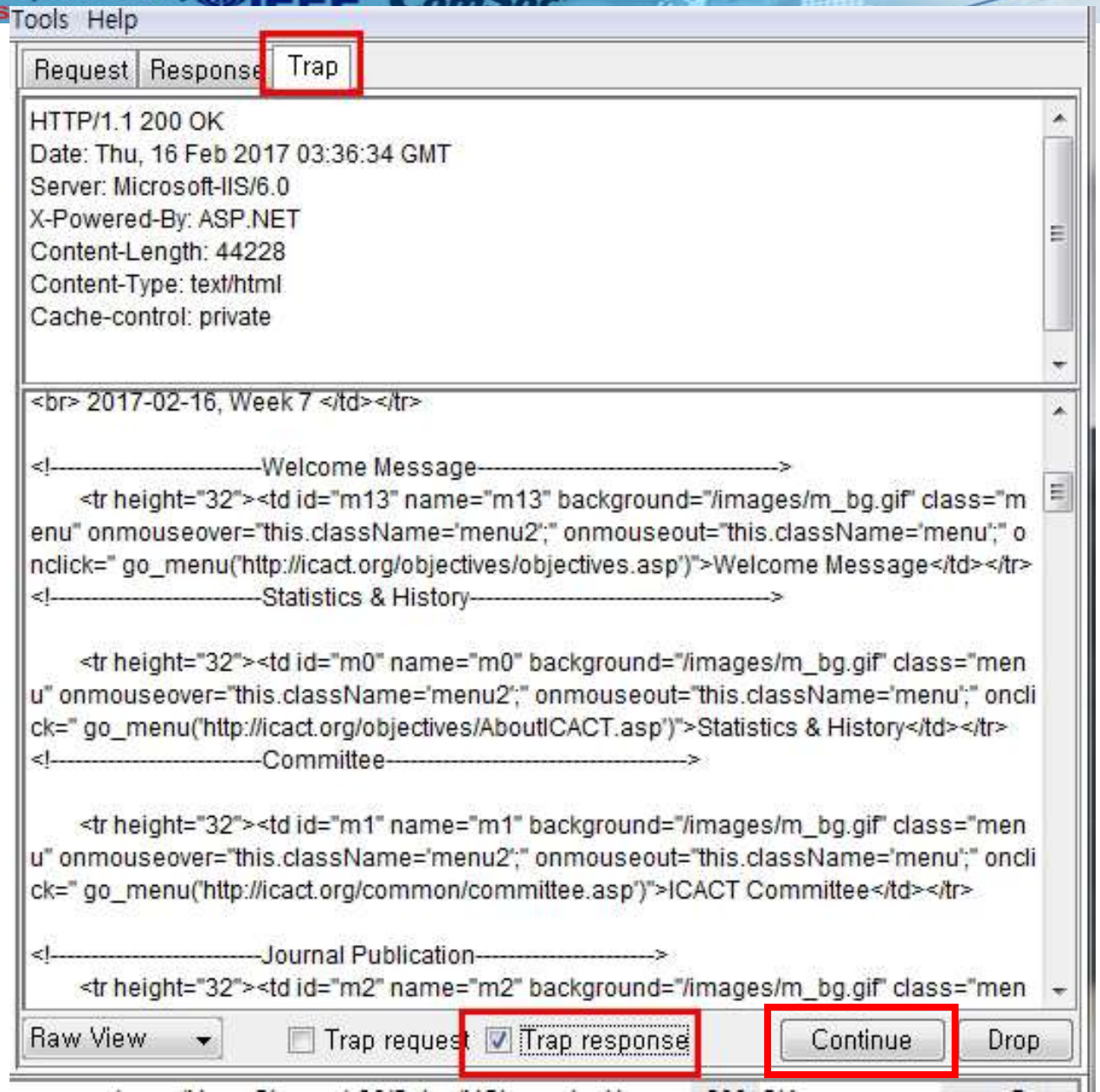




Paros intercept & modify HTTP Data



Paros intercept & modify HTTP Data



Paros Demonstration !

http://www.skku.edu/index_pc.jsp >>global
http://www.skku.edu/eng_home/index.jsp

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

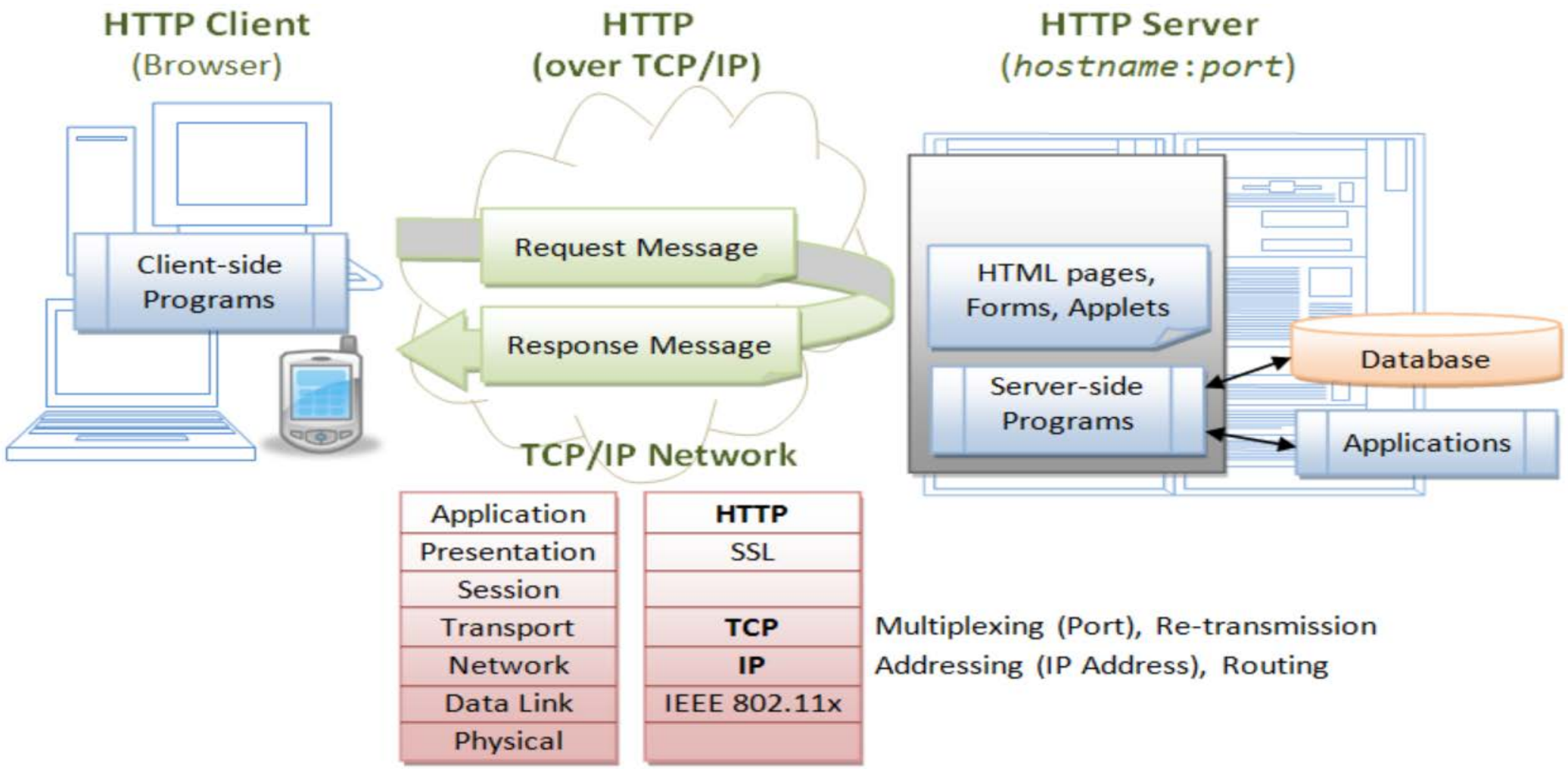
GET http://admission-global.skku.edu/admission/undergraduate/schedule.jsp HTTP/1.1

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 !



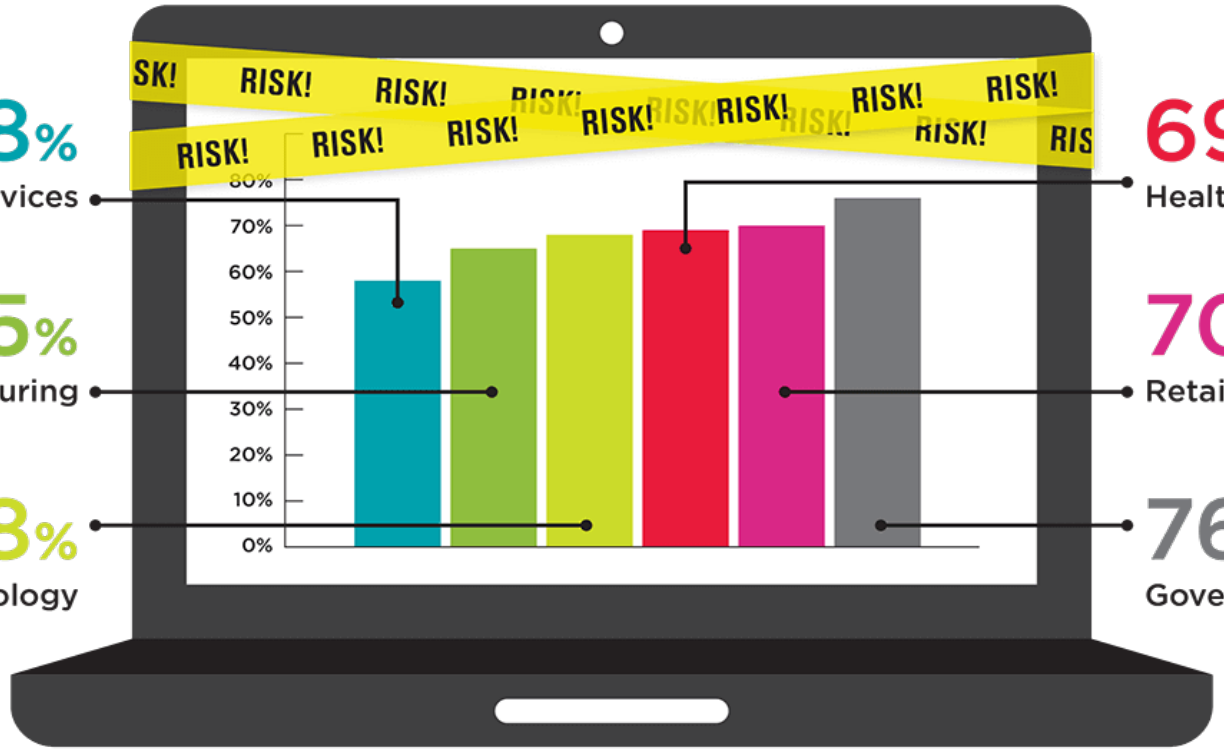
Web Hacking & Defensing! - OWASP top 10 vulnerabilities

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?



Financial — 58% Financial Services

Manufacture — 65% Manufacturing

Technology — 68% Technology

69% Healthcare — **Healthcare**

70% Retail + Hospitality — **Retail**

76% Government — **Government**

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.

VERACODE