

COMPUTER SYSTEMS SECURITY

Lab Session 03

Explore Web tracking

Name: Syeda Marium Faheem

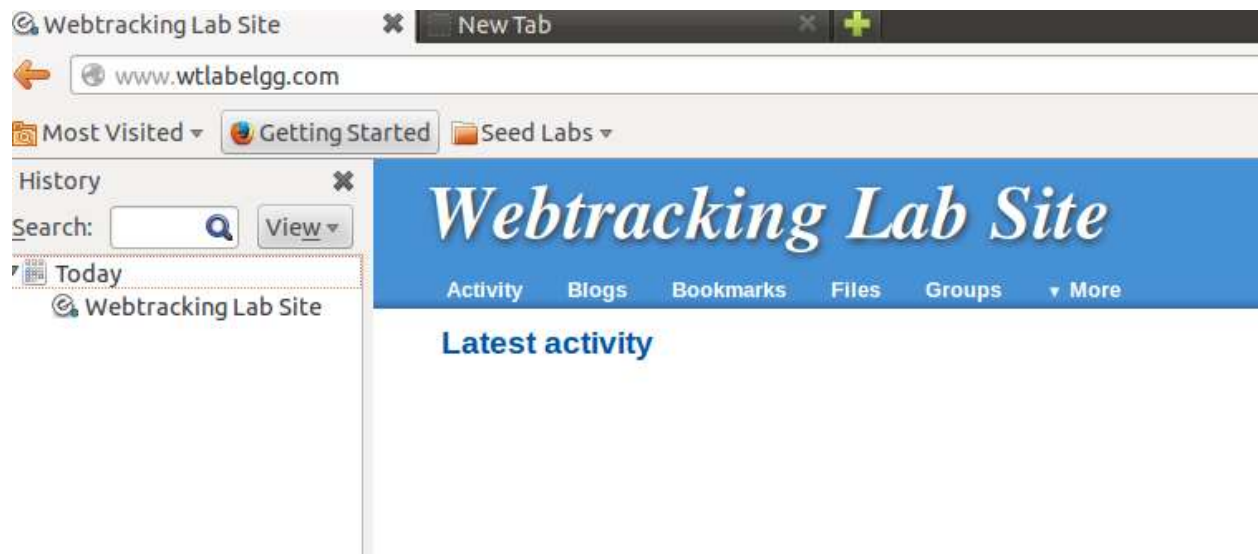
Roll No: CS-099

Section: B

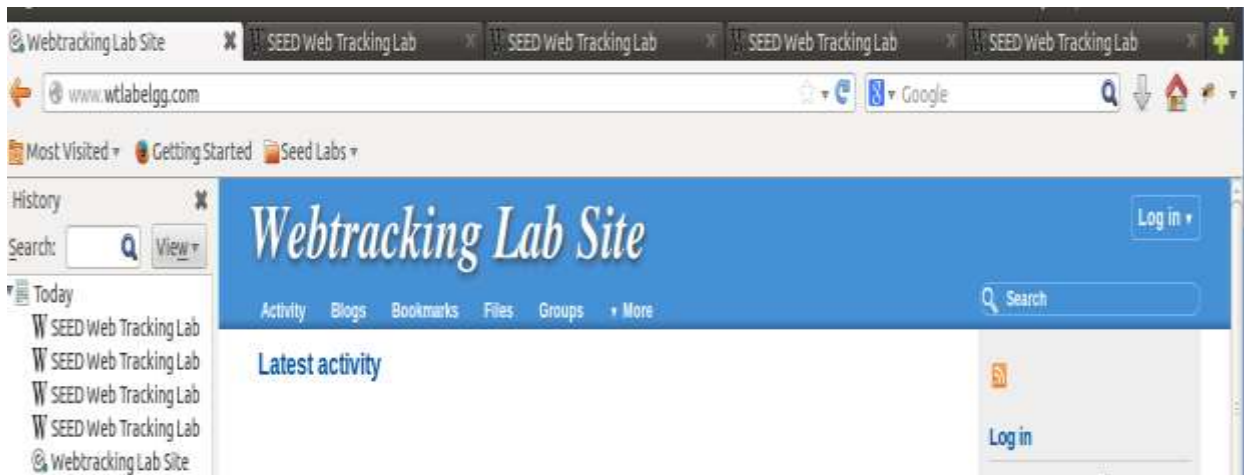
Task No.1



Now Open <http://www.wtlabelgg.com>.



In Webtracking, recent activity added



Recent Click item added on front page of Webtracking Lab Site

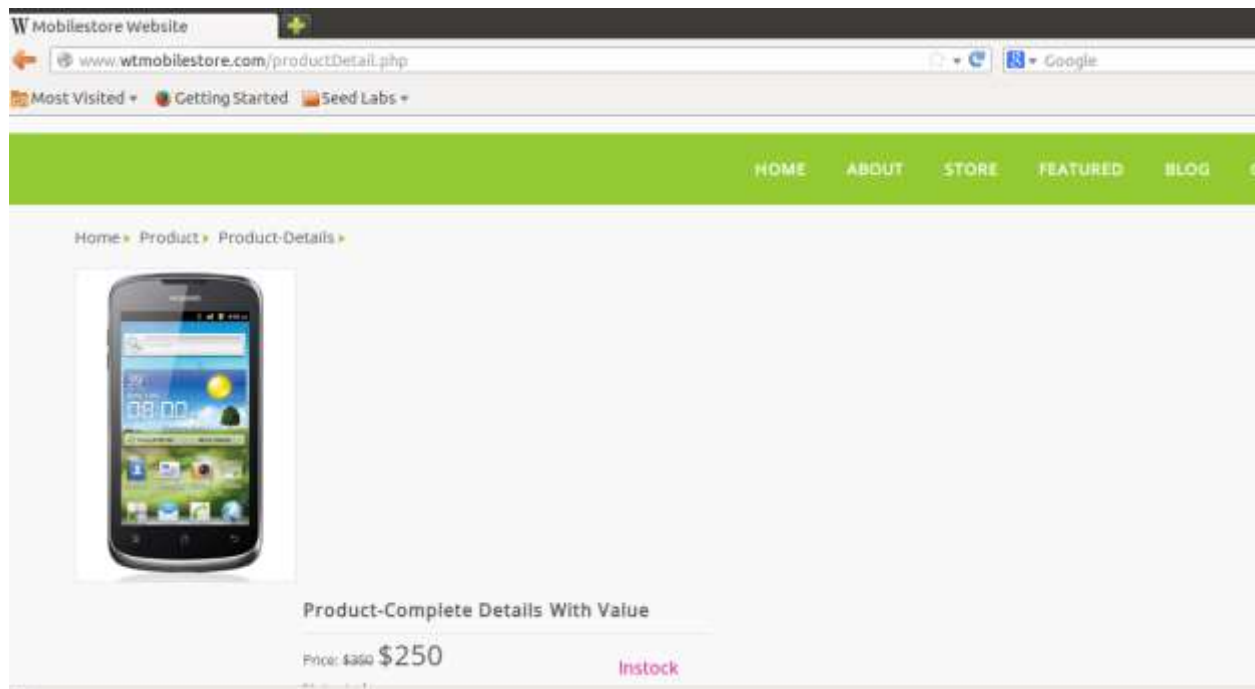


Webs tracking basically make track of recent click items or product on it main page.

Task No.2:

Since ,Third party cookies are cookies that are set by web site with a domain name other than the one the user is currently visiting. For example, user visits website abc.com, say the web page abc.com has an image to fetch from xyz.com. That image request can set cookie on domain xyz.com, and the cookie set on xyz.com domain is known as a third-party cookie. Some advertisers use these types of cookies to track your visits to the various websites on which they advertise.

I opened :



So cookies of third party will be;

<http://fonts.googleapis.com/css?family=Londrina+Solid|Coda+Caption:800|Open+Sans>

GET /css?family=Londrina+Solid|Coda+Caption:800|Open+Sans HTTP/1.1

Host: fonts.googleapis.com

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:23.0) Gecko/20100101 Firefox/23.0

Accept: text/css,*/*;q=0.1

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer: http://www.wtmobilestore.com/productDetail.php

Connection: keep-alive

HTTP/1.1 200 OK

Content-Type: text/css; charset=utf-8

Access-Control-Allow-Origin: *

Timing-Allow-Origin: *

Expires: Thu, 03 Sep 2020 13:28:36 GMT

Date: Thu, 03 Sep 2020 13:28:36 GMT

Cache-Control: private, max-age=86400

Content-Encoding: gzip

Transfer-Encoding: chunked

Server: ESF

X-XSS-Protection: 0

X-Frame-Options: SAMEORIGIN

X-Content-Type-Options: nosniff

http://www.wtlabadsrver.com/track.php?guid=8326918373014243

GET /track.php?guid=8326918373014243 HTTP/1.1

Host: www.wtlabadsrver.com

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:23.0) Gecko/20100101 Firefox/23.0

Accept: image/png,image/*;q=0.8,*/*;q=0.5

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer: http://www.wtmobilestore.com/productDetail.php

Cookie: track=4075642969650095

Connection: keep-alive

HTTP/1.1 200 OK

Date: Thu, 03 Sep 2020 13:28:36 GMT

Server: Apache/2.2.22 (Ubuntu)

X-Powered-By: PHP/5.3.10-1ubuntu3.14

Vary: Accept-Encoding

Content-Encoding: gzip

Content-Length: 21

Keep-Alive: timeout=5, max=100

Connection: Keep-Alive

Content-Type: text/html

http://www.wtlabadsrver.com/track.php?guid=8326918373014243

GET /track.php?guid=8326918373014243 HTTP/1.1

Host: www.wtlabadsrver.com

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:23.0) Gecko/20100101 Firefox/23.0

Accept: image/png,image/*;q=0.8,*/*;q=0.5

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer: http://www.wtmobilestore.com/productDetail.php

Cookie: track=4075642969650095

Connection: keep-alive

HTTP/1.1 200 OK

Date: Thu, 03 Sep 2020 13:28:37 GMT

Server: Apache/2.2.22 (Ubuntu)

X-Powered-By: PHP/5.3.10-1ubuntu3.14

Vary: Accept-Encoding

Content-Encoding: gzip

Content-Length: 21

Keep-Alive: timeout=5, max=99

Connection: Keep-Alive

Content-Type: text/html

http://safebrowsing.clients.google.com/safebrowsing/downloads?client=Firefox&appver=23.0&pver=2.2&wrkey=AKEgNivjELzZykoNghtMu6vIXHFZr7PkCnpnCxxCIS-G2XN46_21pc_e...
POST /safebrowsing/downloads?client=Firefox&appver=23.0&pver=2.2&wrkey=AKEgNivjELzZykoNghtMu6vIXHFZr7PkCnpnCxxCIS-G2XN46_21pc_euMILLtFf0rFqN7gA3M-fCBmRshy...
Host: safebrowsing.clients.google.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:23.0) Gecko/20100101 Firefox/23.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Length: 4086
Content-Type: text/plain
Cookie: NiD=204=NaTXiLLv9JaBXdlVSj366i8BO6_t_Awu_3ru_P_tv7GosO1qKLL-19H9hjhiZxjh_X_2uxrAur5hVxJNMY_7loZJbXUsp3NWlNTv6oOGT1FAn1wAvv4ZgFX9ZY72v8ATWUXSEC...
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
goog-melware-shavar;a:220711-22549B:s:214080,214082-214086,214088-214093,214095-214127,214129-214138,214140-214147,214150-214155,214157-214172,214174-214179,2141...
goog-phish-shavar;a:427789-430166:s:248177,248179,248181,248184,248186-248188,248193-248198,248201-248202,248204-248206,248208-248209,248211-248216,248219-248221,...

HTTP/1.1 403 Forbidden
Content-Length: 1103
Content-Type: text/html; charset=UTF-8
Date: Thu, 03 Sep 2020 13:28:38 GMT
Connection: close

http://fonts.gstatic.com/s/opensans/v17/mem8YaGs126MiZpBA-UfVZ0d.woff

GET /s/opensans/v17/mem8YaGs126MiZpBA-UfVZ0d.woff HTTP/1.1
Host: fonts.gstatic.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:23.0) Gecko/20100101 Firefox/23.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://fonts.googleapis.com/css?family=Londrina+Solid|Coda+Caption:800|Open+Sans
Origin: http://www.wtmobilestore.com
Connection: keep-alive

HTTP/1.1 200 OK
Accept-Ranges: bytes
Content-Type: font/woff
Access-Control-Allow-Origin: *
Timing-Allow-Origin: *
Content-Length: 18100
Date: Tue, 01 Sep 2020 07:34:20 GMT
Expires: Wed, 01 Sep 2021 07:34:20 GMT
Last-Modified: Tue, 23 Jul 2019 19:30:45 GMT
X-Content-Type-Options: nosniff
Server: sffe

X-XSS-Protection: 0

Age: 104058


```
http://safebrowsing.clients.google.com/safebrowsing/downloads?client=Firefox&appver=23.0&pver=2.2&wrkey=AKEgNivjELzZykoNghtMu6vXHFZz7PkCnpnCxsCIS-G2XN46_21pc_e...

POST /safebrowsing/downloads?client=Firefox&appver=23.0&pver=2.2&wrkey=AKEgNivjELzZykoNghtMu6vXHFZz7PkCnpnCxsCIS-G2XN46_21pc_euMILtFQrFqN7gA3M-fC8mRshy...
Host: safebrowsing.clients.google.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:23.0) Gecko/20100101 Firefox/23.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Length: 4086
Content-Type: text/plain
Cookie: NID=204=NaTX8Lv9Ja8XdIV5j566i8BO6_t_Awu_3ru_P_tv7GosOT1qKLL-19H9PqNixh_X_2uxrAur5hVxJNMY_7ioZjbXUsp3NWINTv6oOGT1FAn1wAVv4ZgFk9ZY72vBAfWUX5EC...
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
goog-malware-shavar:a:220711-225498:s:214080,214082-214086,214088-214093,214095-214127,214129-214138,214140-214147,214150-214155,214157-214172,214174-214179,2141...
goog-phish-shavar:a:427789-430166:s:248177,248179,248181,248184,248186-248188,248193-248198,248201-248202,248204-248206,248208-248209,248211-248216,248219-248221,...

HTTP/1.1 403 Forbidden
Content-Length: 1103
Content-Type: text/html; charset=UTF-8
Date: Thu, 03 Sep 2020 13:29:39 GMT
Connection: close
```

<http://ocsp.digicert.com/>

POST / HTTP/1.1

Host: ocsp.digicert.com

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:23.0) Gecko/20100101 Firefox/23.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Content-Length: 115

Content-Type: application/ocsp-request

Connection: keep-alive

OqOo0M0K0IO+

HTTP/1.1 200 OK

Accept-Ranges: bytes

Age: 4486

Cache-Control: max-age=158955

Content-Type: application/ocsp-response

Date: Thu, 03 Sep 2020 13:32:32 GMT

Etag: "5f50a8d5-1d7"

Expires: Sat, 05 Sep 2020 09:41:47 GMT

Last-Modified: Thu, 03 Sep 2020 08:27:01 GMT

Server: ECS (uae/9153)

X-Cache: HIT

```
https://versioncheck-bg.addons.mozilla.org/update/VersionCheck.php?reqVersion=2&id=firefox-hotfix@mozilla.org&version=20140527.01.3&maxAppVersion=%ITEM_MAXAPPE...

GET /update/VersionCheck.php?reqVersion=2&id=firefox-hotfix@mozilla.org&version=20140527.01.3&maxAppVersion=%ITEM_MAXAPPE...
Host: versioncheck-bg.addons.mozilla.org
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:23.0) Gecko/20100101 Firefox/23.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: sessionId=.eJwNxBENGDAIAMBdmACEAnUzgy0sYB8mxt31fvdA3XFck1bCDhKeVnIOR8yQydVsNHZDUnP7q1E2NaiYukdi3yjfSEIq04T3A70ZFk0:1kAhi2:0r2zs1f9CZNebs-hvnCl6...
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache

HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 2
Connection: keep-alive
Cache-Control: max-age=3600
content-security-policy: default-src 'none'; object-src 'none'; report-uri /__cspreport__
Date: Thu, 03 Sep 2020 12:42:29 GMT
Expires: Thu, 03 Sep 2020 13:42:29 GMT
Last-Modified: Thu, 03 Sep 2020 12:42:29 GMT
Public-Key-Pins: max-age=5184000; includeSubDomains; pin-sha256="woIwRyIOVNa9ihaBcIRSC7Xqf@Y59VwUGOlud4PB18="; pin-sha256="r/mikG3eEpVdm+u/ko/cwxzOMo1bk4TyHIL...
Server: nginx
```

```
https://services.addons.mozilla.org/en-US/firefox/api/1.5/search/guid:langpack-en-ZA%40firefox.mozilla.org,langpack-en-GB%40firefox.mozilla.org,%7B972ce4c6-7e08-4474-a285-...

GET /en-US/firefox/api/1.5/search/guid:langpack-en-ZA%40firefox.mozilla.org,langpack-en-GB%40firefox.mozilla.org,%7B972ce4c6-7e08-4474-a285-3208198ce0fd%7D,ubufu%40u...
Host: services.addons.mozilla.org
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:23.0) Gecko/20100101 Firefox/23.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: sessionId=.eJwNxBENGDAIAMBdmACEAnUzgy0sYB8mxt31fvdA3XFck1bCDhKeVnIOR8yQydVsNHZDUnP7q1E2NaiYukdi3yjfSEIq04T3A70ZFk0:1kAhi2:0r2zs1f9CZNebs-hvnCl6...
Connection: keep-alive

HTTP/1.1 404 Not Found
Content-Encoding: gzip
content-security-policy: child-src 'self' https://www.google.com/recaptcha/ https://www.recaptcha.net/recaptcha/; media-src https://videos.cdn.mozilla.net; object-src 'none'; imgs...
Content-Type: text/html; charset=utf-8
Date: Thu, 03 Sep 2020 13:32:33 GMT
Etag: W/"47177e183db261240d4adb075d147c03"
Server: nginx
Strict-Transport-Security: max-age=31536000
Vary: Accept-Encoding
X-AMO-Request-ID: 8f5033cb5c824d6aa56ab11e081b1ca2
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
```

```
https://blocklist.addons.mozilla.org/blocklist/3/%7Bec8030f7-c20a-464f-9b0e-13a3a9e97384%7D/23.0/Firefox/20130803193343/Linux_x86-gcc3/en-US/release/Linux%203.5.0-37-ge...

GET /blocklist/3/%7Bec8030f7-c20a-464f-9b0e-13a3a9e97384%7D/23.0/Firefox/20130803193343/Linux_x86-gcc3/en-US/release/Linux%203.5.0-37-generic%20(GTK%202.24.10)/cano...
Host: blocklist.addons.mozilla.org
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:23.0) Gecko/20100101 Firefox/23.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
Cookie: sessionId=.eJwNxBENGDAIAMBdmACEAnUzgy0sYB8mxt31fvdA3XFck1bCDhKeVnIOR8yQydVsNHZDUnP7q1E2NaiYukdi3yjfSEIq04T3A70ZFk0:1kAhi2:0r2zs1f9CZNebs-hvnCl6...
Connection: keep-alive

HTTP/1.1 301 Moved Permanently
Content-Type: text/html
Content-Length: 178
Connection: keep-alive
content-security-policy: default-src 'none'; object-src 'none'; report-uri /__cspreport__
Date: Thu, 03 Sep 2020 13:34:34 GMT
Location: https://blocklists.settings.services.mozilla.com/v1/blocklist/3/%7Bec8030f7-c20a-464f-9b0e-13a3a9e97384%7D/23.0/Firefox/20130803193343/Linux_x86-gcc3/en-US/rele...
Server: nginx
Strict-Transport-Security: max-age=300
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
```

Now View page-source

request for tracking cookie.

```
</div>
</div>
<div class="clear">
  
</div>
<div class="footer">
  <div class="wrap">
    <div class="section group">
      <div class="col_1_of_4 span_1_of_4">
        <h3>Our Info</h3>
        <p>Lorem ipsum dolor sit amet, consectetur adipisicing elit, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo</p>
      </div>
      <div class="col_1_of_4 span_1_of_4">
        <h3>Latest News</h3>
        <p>Lorem ipsum dolor sit amet, consectetur adipisicing elit.</p>
        <p>Lorem ipsum dolor sit amet, consectetur adipisicing elit.</p>
        <p>Lorem ipsum dolor sit amet, consectetur adipisicing elit.</p>
      </div>
      <div class="col_1_of_4 span_1_of_4">
        <h3>Store Location</h3>
        <p>Lorem ipsum dolor sit amet, consectetur adipisicing elit.</p>
        <h3>Order online</h3>
        <p>080-1234-56789</p>
        <p>080-1234-56780</p>
      </div>
    </div>
  </div>
</div>
</div>
</div>
```

Now open <http://www.wtshoestore.com/>

W Shoestore Website


www.wtshoestore.com/productDetail.php

Google

Most Visited Getting Started Seed Labs

HOME ABOUT STORE FEATURE

Home Product Product-Details



Product-Complete Details With Value

Price: ~~\$350~~ **\$250**

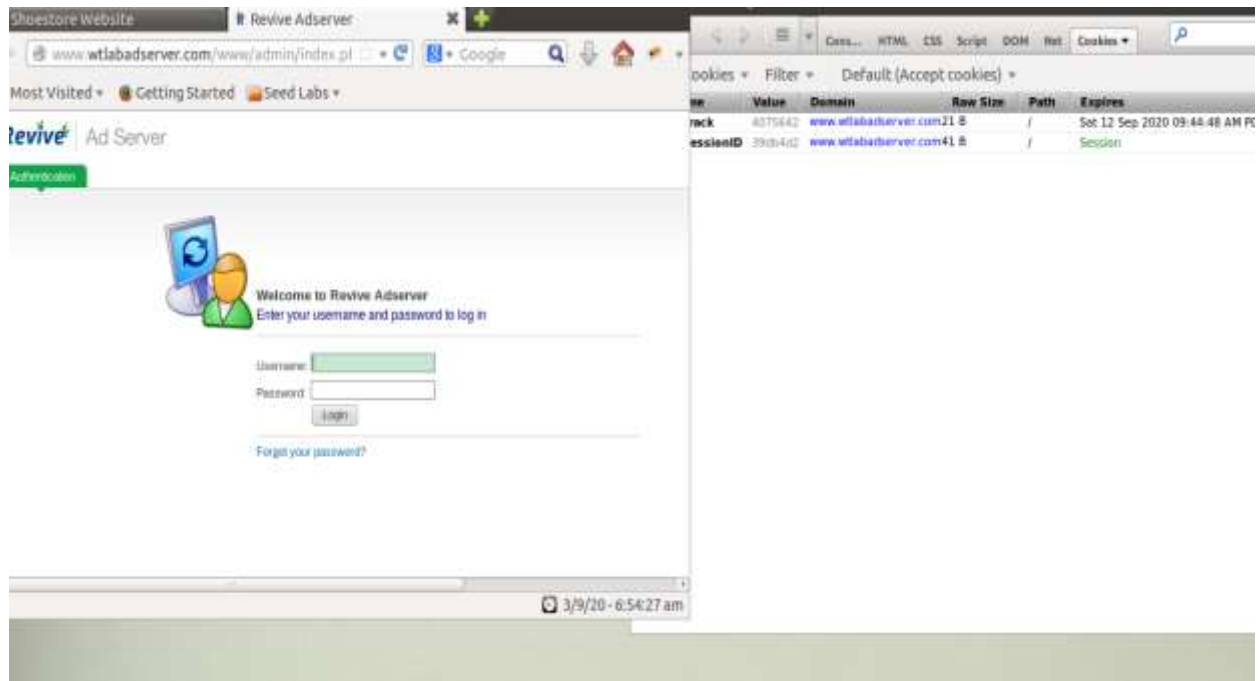
Instock

Not rated

No reviews

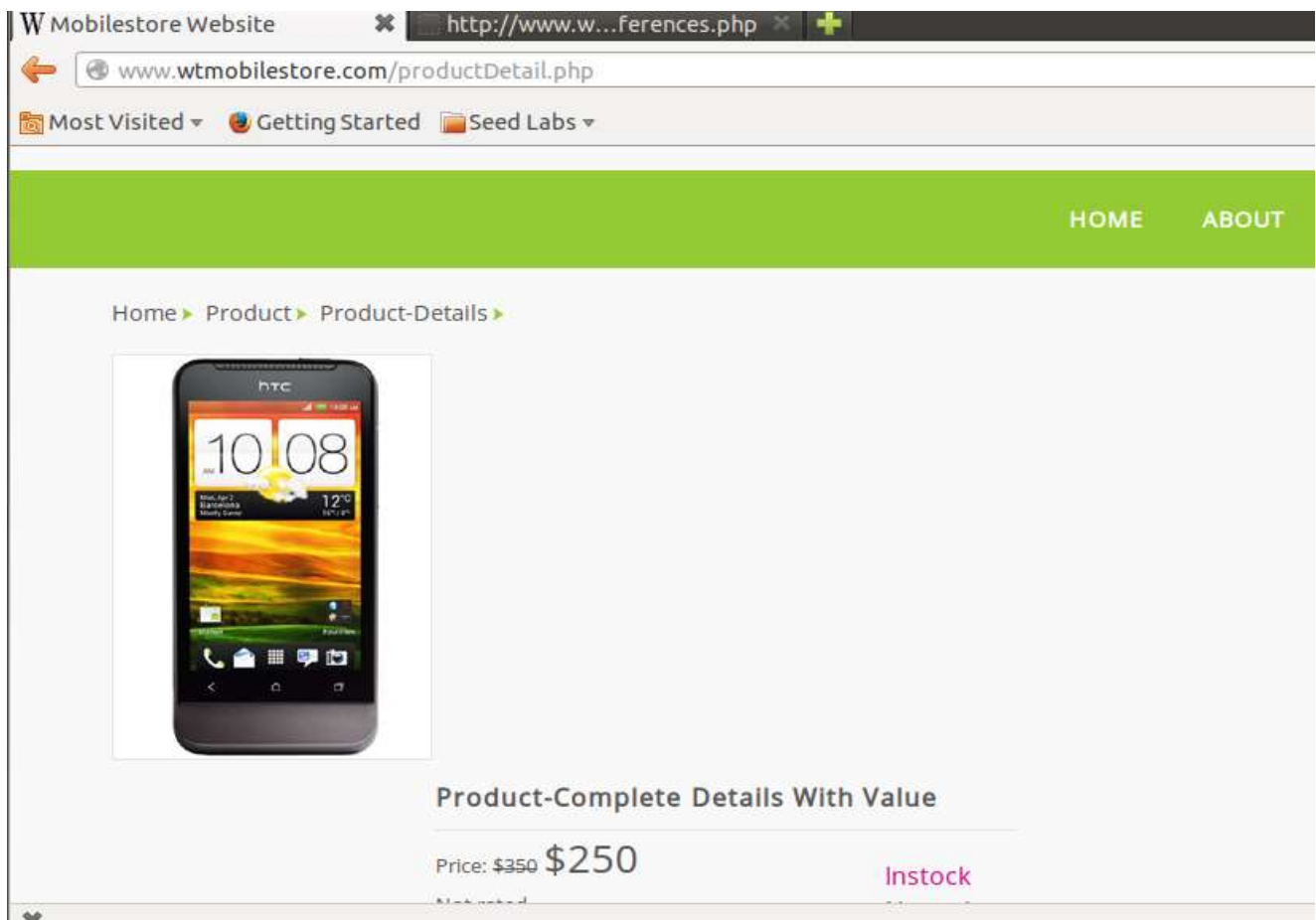
Description :

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute inure



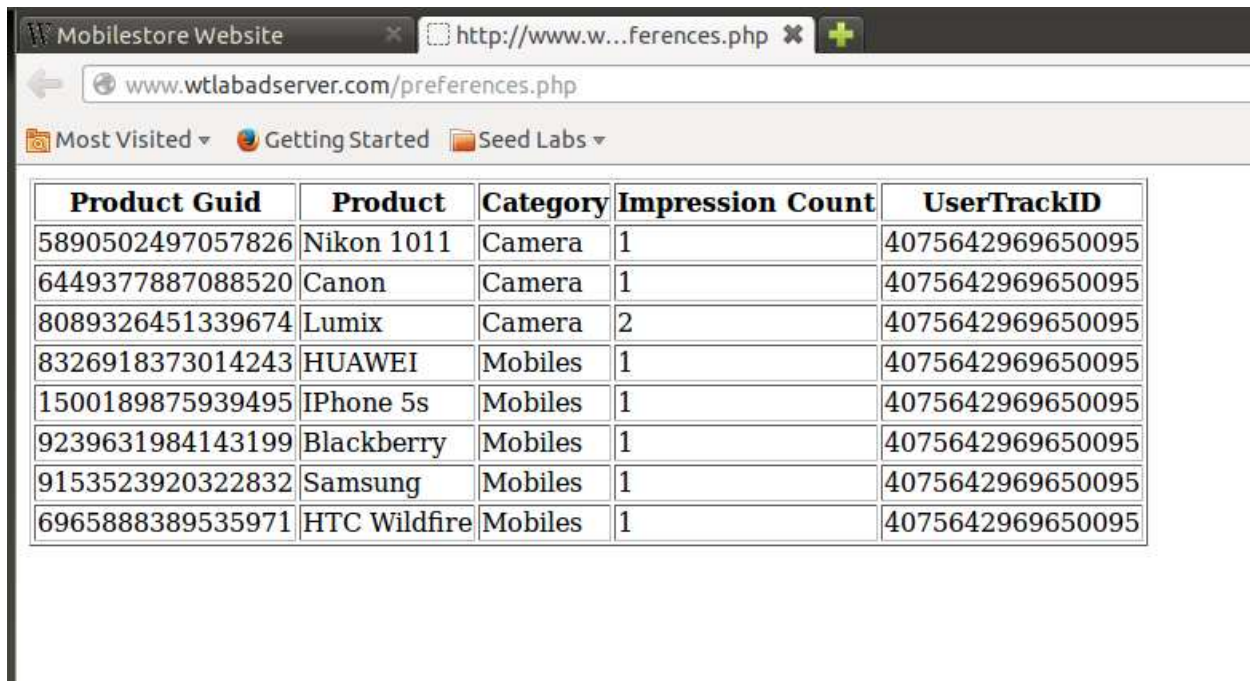
Task no.3

Open wtmobilestore.com , click on item get so



www.wtlabserver.com/preferences.php: This page basically record or maintain track of visited website and their items like it basically count click and impression . this page continuously maintain track of

all clicks and impression



Product Guid	Product	Category	Impression Count	UserTrackID
5890502497057826	Nikon 1011	Camera	1	4075642969650095
6449377887088520	Canon	Camera	1	4075642969650095
8089326451339674	Lumix	Camera	2	4075642969650095
8326918373014243	HUAWEI	Mobiles	1	4075642969650095
1500189875939495	IPhone 5s	Mobiles	1	4075642969650095
9239631984143199	Blackberry	Mobiles	1	4075642969650095
9153523920322832	Samsung	Mobiles	1	4075642969650095
6965888389535971	HTC Wildfire	Mobiles	1	4075642969650095

Task No.4

<http://www.wtlabserver.com/displayads.php>

GET /displayads.php HTTP/1.1

Host: www.wtlabserver.com

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:23.0) Gecko/20100101 Firefox/23.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer: http://www.wtlabserver.com/

Cookie: track=4075642969650095

Connection: keep-alive

HTTP/1.1 200 OK

Date: Wed, 02 Sep 2020 17:43:58 GMT

Server: Apache/2.2.22 (Ubuntu)

X-Powered-By: PHP/5.3.10-1ubuntu3.14

Vary: Accept-Encoding

Content-Encoding: gzip

Content-Length: 115

Keep-Alive: timeout=5, max=100

Connection: Keep-Alive

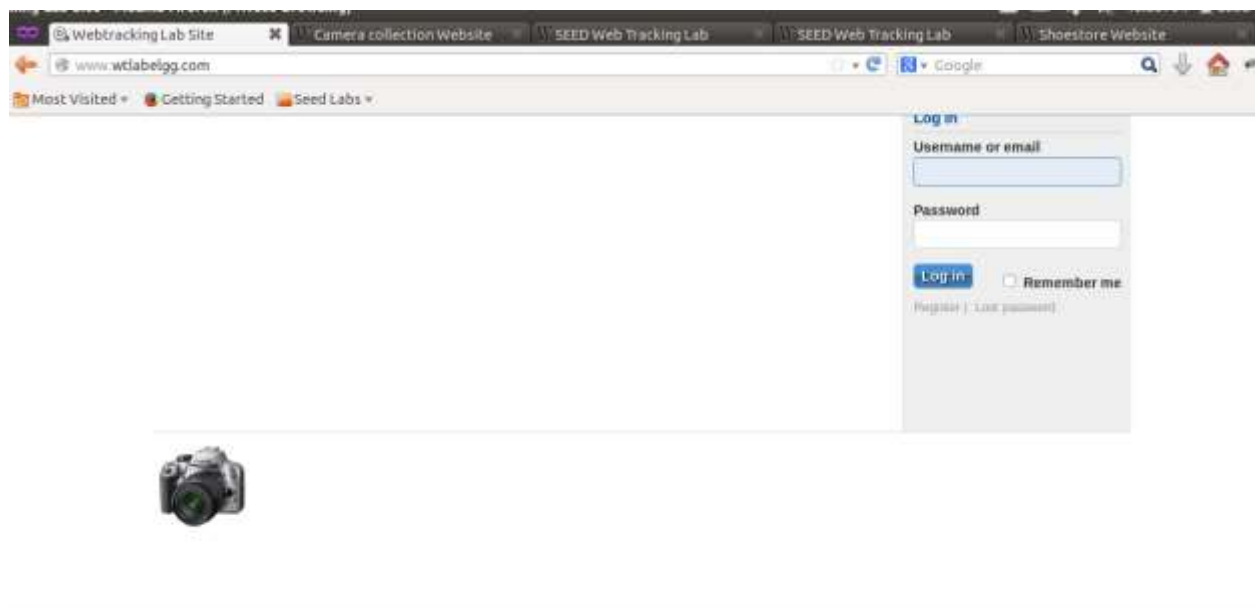
Content-Type: text/html

http://www.wtlabadsrver.com/www/images/c569cf62c790549e342557b7054b539c.jpg

GET /www/images/c569cf62c790549e342557b7054b539c.jpg HTTP/1.1
Host: www.wtlabadsrver.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:23.0) Gecko/20100101 Firefox/23.0
Accept: image/png,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.wtlabadsrver.com/displayads.php
Cookie: track=4075642969650095
Connection: keep-alive

HTTP/1.1 200 OK
Date: Wed, 02 Sep 2020 17:43:58 GMT
Server: Apache/2.2.22 (Ubuntu)
Last-Modified: Wed, 17 Sep 2014 08:24:04 GMT
Etag: "2e2d25-5d94-5033e97439251"
Accept-Ranges: bytes
Content-Length: 23956
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: image/jpeg

Task No.5



Every time on refresh it store only current item although in task no 1. All item that were click shown here

Task No.6:

▼ General

Request URL: <https://www.dictionary.com/>

Request Method: GET

Status Code: 🟢 304

Remote Address: 151.101.2.133:443

Referrer Policy: no-referrer-when-downgrade

▼ Response Headers

accept-ranges: bytes

Access-Control-Allow-Methods: GET, PUT, POST, DELETE, HEAD, OPTIONS

Access-Control-Allow-Origin: <https://www.dictionary.com>

adler-geo: ROWLOatlantic

age: 3133

cache-control: max-age=3600, public

content-encoding: gzip

content-length: 35597

content-security-policy: upgrade-insecure-requests

content-type: text/html; charset=utf-8

date: Thu, 03 Sep 2020 14:23:25 GMT

etag: W/"2bff0-LZCP5mIoQuELlsAIDmOqkojyOjU"

is-eu: false

platform: Desktop

server: nginx/1.16.1

status: 304

vary: Accept-Encoding, is-eu, is-us, platform, adler-geo, x-variation, X-OPTIONS

via: 1.1 varnish

x-cache: HIT

x-cache-hits: 21

x-powered-by: Express

x-served-by: cache-sin18041-SIN

x-timer: S1599143806.966077,V50,V61

x-variation: v0

▼ Request Headers

:authority: www.dictionary.com

:method: GET

:path: /

:scheme: https

accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9


```
accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
accept-encoding: gzip, deflate, br
accept-language: en-US,en;q=0.9
cache-control: max-age=0
cookie: sid=937936-1599142907483; sid=935258-159686688226; Variation=v0; _gcl_id=1.1.37848826.1599142908; _ga=GA1.2.2093054367.1599142908; _gid=GA1.2.786486771.1599142908; salitr_u_p
ageviews=1; _fbp=fb.1.1599142907483.317835489; salitr_u_visitor=8c803473-7465-44f1-9123-9e52859a4071; __gads=ID=89281cc966b5a4a9-222a34e311e600ed(T=1599142911;RT=1599142911;S=ALNT_MaX
NzIR1A=9dFqenK1IxaFjIRANQ; OptanonConsent=laIAR01oba1=faias&datatemp=Thu-Sep-03-2020-19N3A22N3AB5+GMTN28D580+(Pakistan+Standard+Time)&version=0.5.0&hosts=&landingPath=http%3A%2F%2F
www.dictionery.com%2F&groups=C0802K3A1N2CC0801N3A1N2CC0805N3A1N2CC0804N3A1
If-none-match: W/"2e4f8-L2CP5eIoQeL1sA1DeOqx0jY05U"
sec-fetch-dest: document
sec-fetch-mode: navigate
sec-fetch-site: cross
sec-fetch-user: ?1

sec-fetch-site: cross
sec-fetch-user: ?1
upgrade-insecure-requests: 1
user-agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83 Safari/537.36
```