Name: Alexey Titov
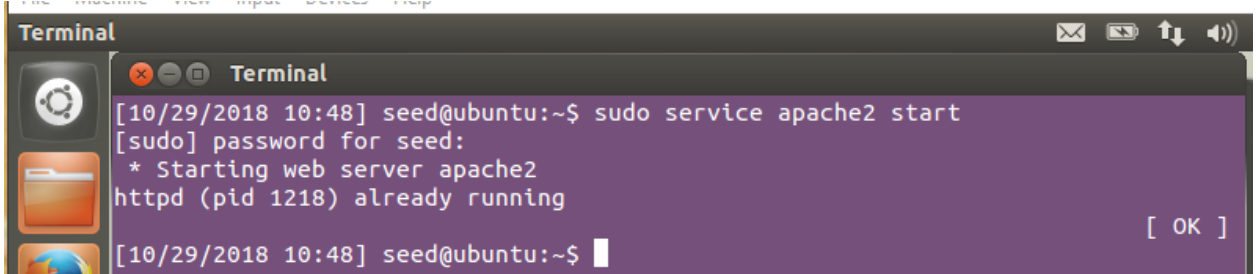
SEEDLabs – Web Tracking Lab (Elgg)

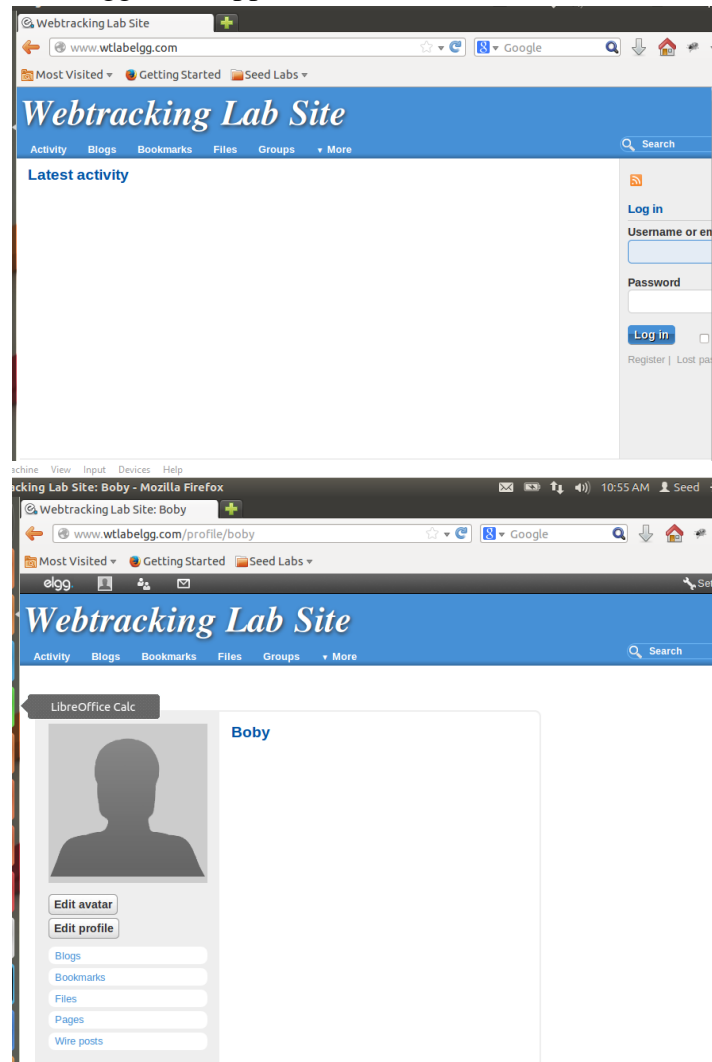## Lab Environment:
- **Environment Configuration:**
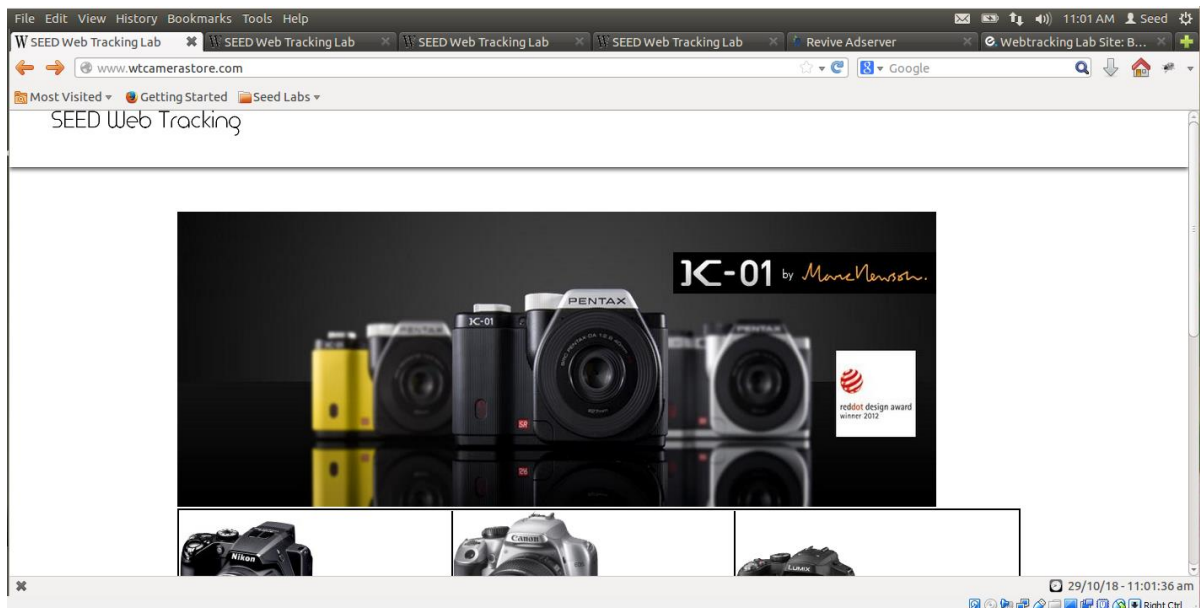 - Starting the Apache Server:

    The Apache Server was started.

  - The Elgg Web Application:

It was observed that all the websites and the logins were working properly.

o   Configuring DNS:

The directory ***/var/www/webtracking/*** contained all the content of the websites.

o   /etc/hosts:

o   Configuring Apache Server:

Each site had a virtual host where the Server name and the document root was provided.

- **Clearing History and cookies:**
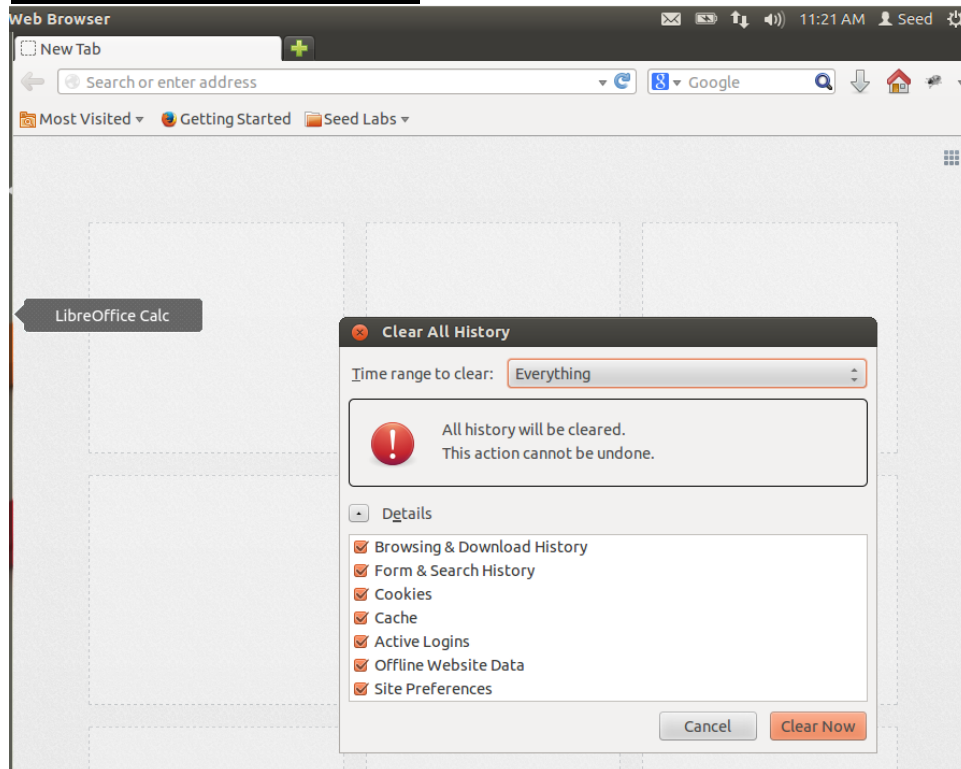
The History was cleared and there were no cookies.

- **Open a new private window in Firefox:**
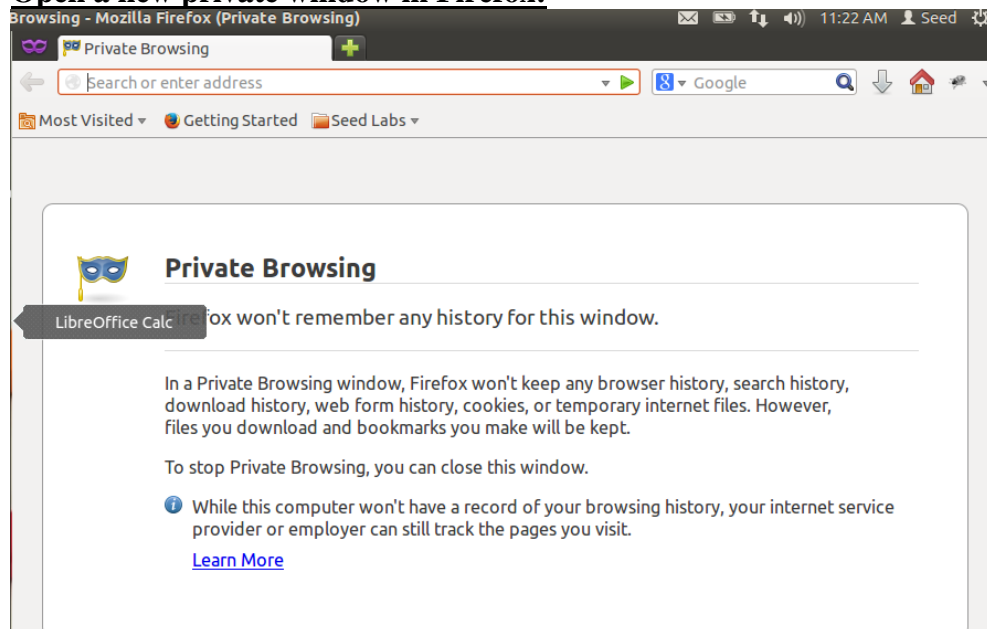
Lab Tasks:

- **Understand the basic working of web tracking**
    1. Open Elgg website without visiting any website and describe your observation in the lab report.
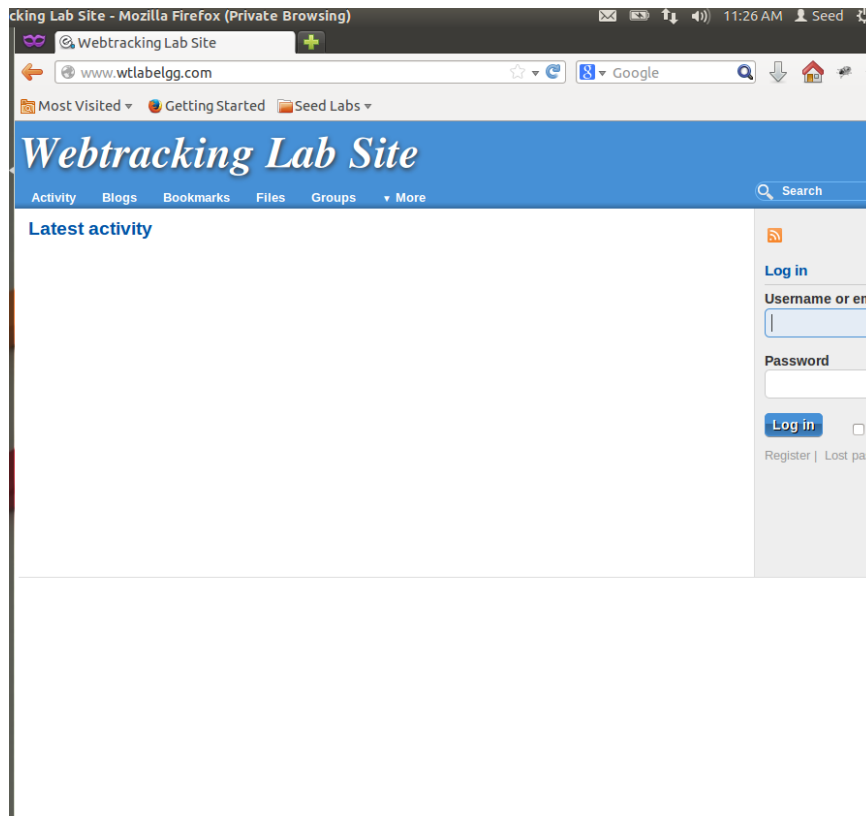
The website www.wtlabelgg.com was blank and was very basic.

2. Open Firefox and open the CameraStore, MobileStore, ElectronicStore and ShoeStore websites.
3. Click on view details for any products in the websites.
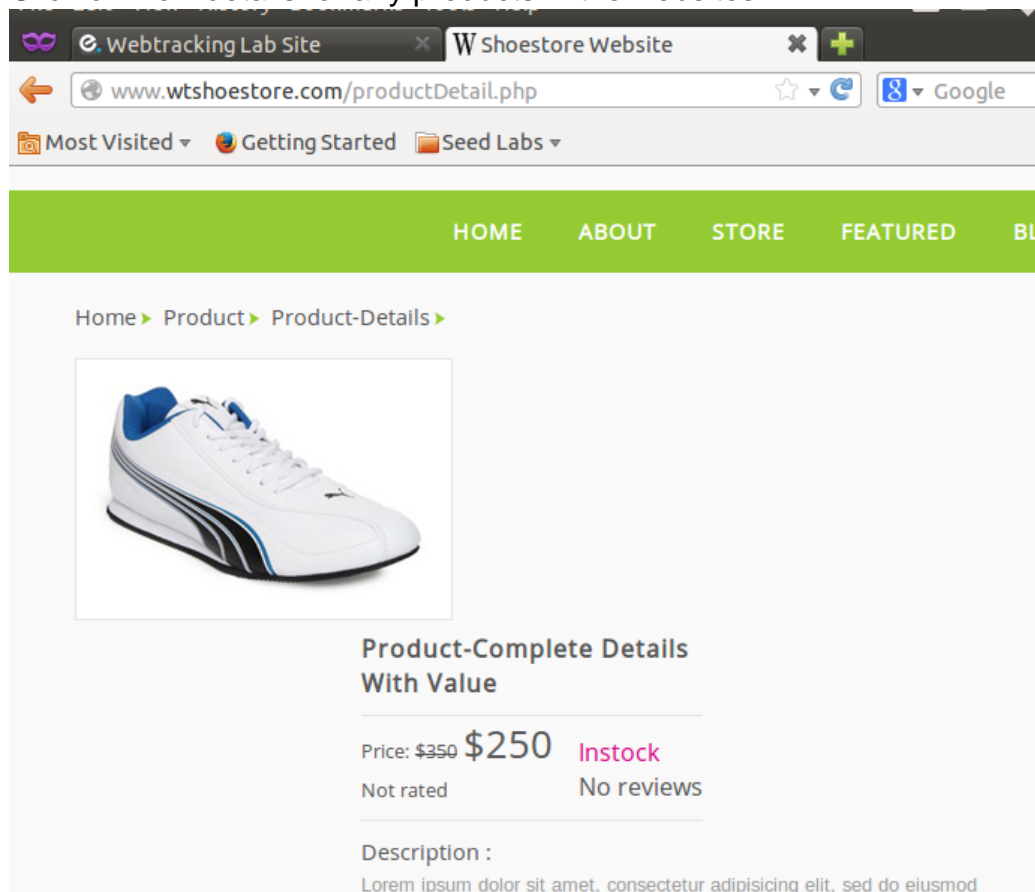
4. Refresh the Elgg website in Firefox and describe your observation.
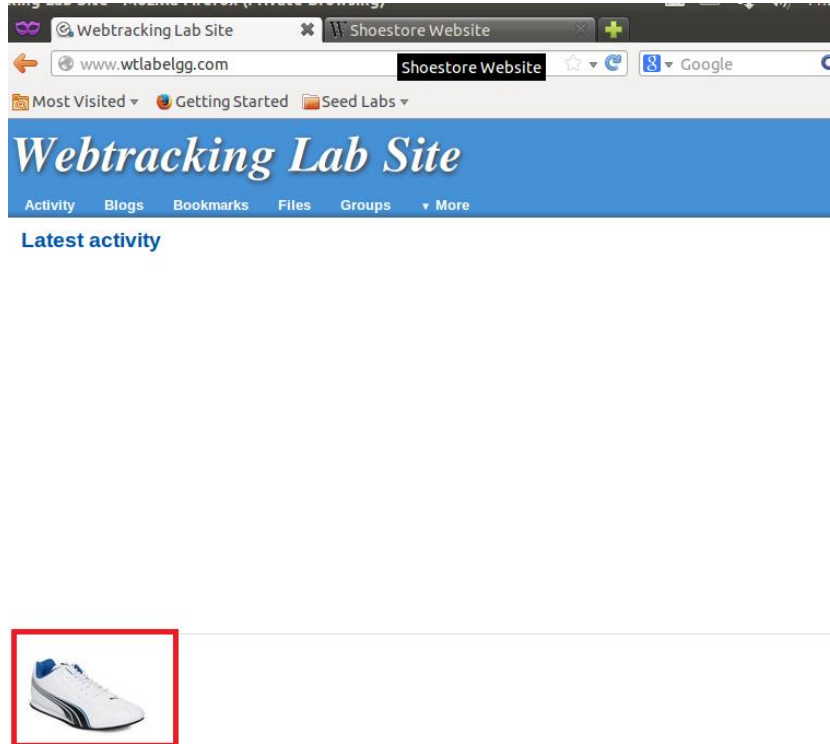
When the Elgg website was refreshed, it showed the product that was recently clicked.

5. Close the browser, reopen it and browse the Elgg website. Describe your observation.

After closing the browser and opening that page again, the ad area was blank.

- **Importance of cookie in Web tracking:**
    1. Open any one of the E Commerce websites CameraStore, MobileStore, ElectronicStore and ShoeStore.
    2. Click on view details for any product in websites and capture LiveHTTPHeader traffic.
    3. In LiveHTTPHeaders, identify the HTTP request, which set the third party cookies, and take the screenshot.
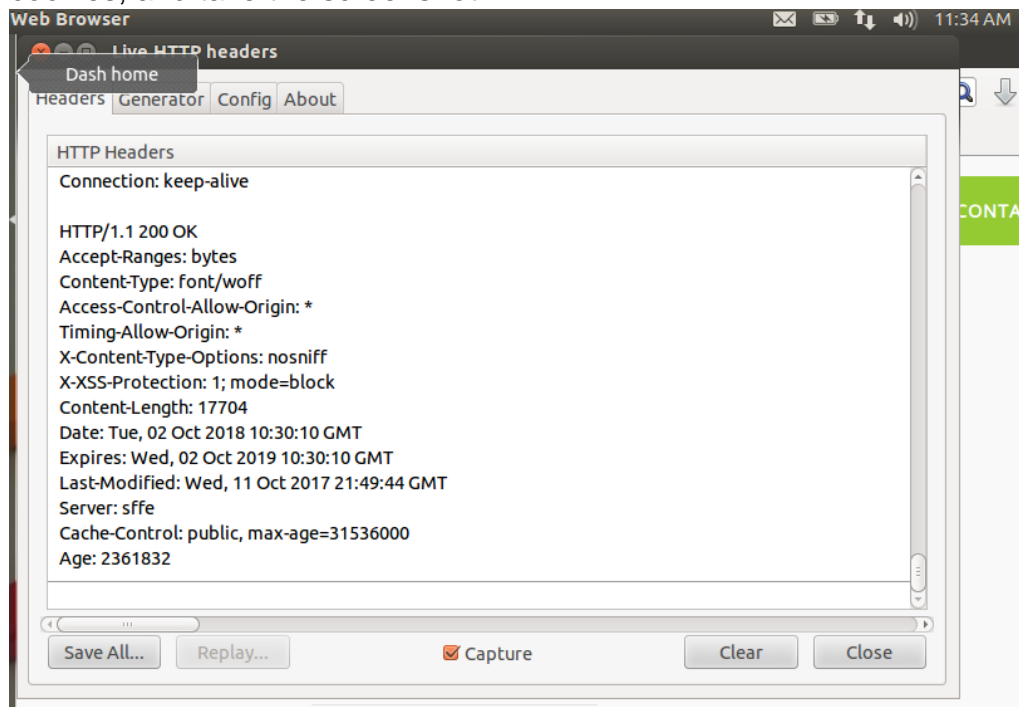
The LiveHTTPHeader was generated as soon as the item was clicked and the website's header information was shown.

    4. Right click on the productDetail page and select View Page Source. Find out how the request for tracking cookie is sent from the webpage, please take a screenshot and describe your observation.
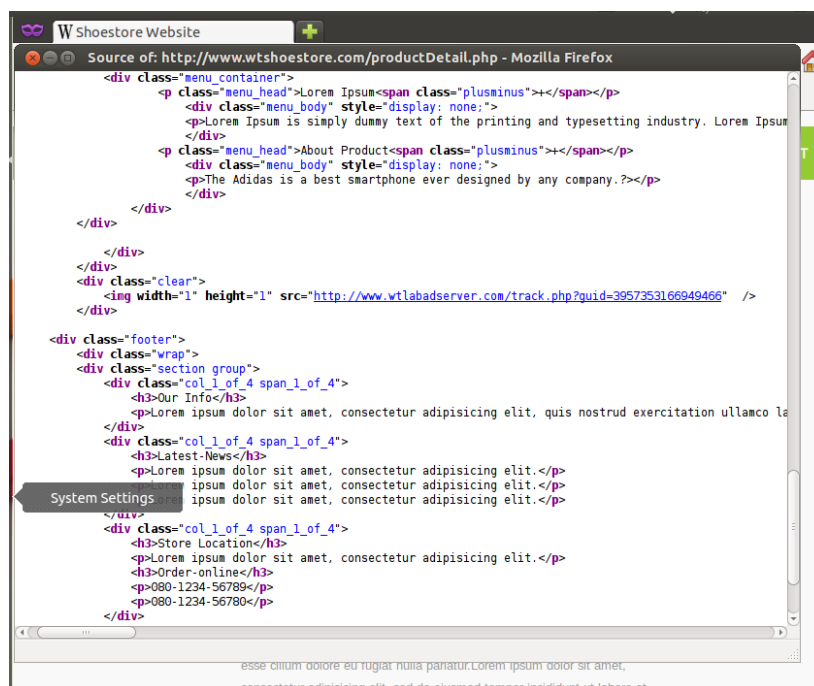
The code line number 130 is where the cookie is sent from the webpage. The website http://www.wtadlabserver.com contains an ad that is served by the Shoestore webpage hence it has set a cookie in the browser. The browser goes to fetch http://www.wtadlabserver.com/ad.html, the response will come back with a Set-Cookie header that sets a cookie with some unique random string.

- **How third party cookies are used in web tracking**
  1. Open any one of the E Commerce websites CameraStore, MobileStore, ElectronicStore, ShoeStore and view details for any product.
  2. Open the ad server web page http://www.wtlabadserver.com
  3. Open Firefox extension Firebug. Observe the Firebug in ad server web page and product web page. Switch between the products webpage and ad server webpage. Describe your observation. (Please do NOT reload the products webpage).
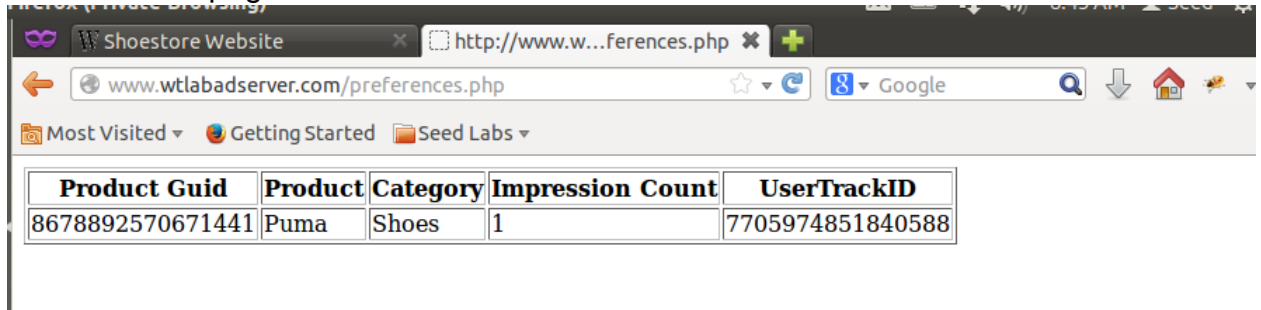
The Firebug extension of the AdServer has an interface of the cookie sent by the Shoestore page. On the other hand the Shoestore page doesn't have that. It's because of the Cookie sent by the page.

- **Tracked user interests and data**
  1. Open the E Commerce websites CameraStore, MobileStore, ElectronicStore and ShoeStore.
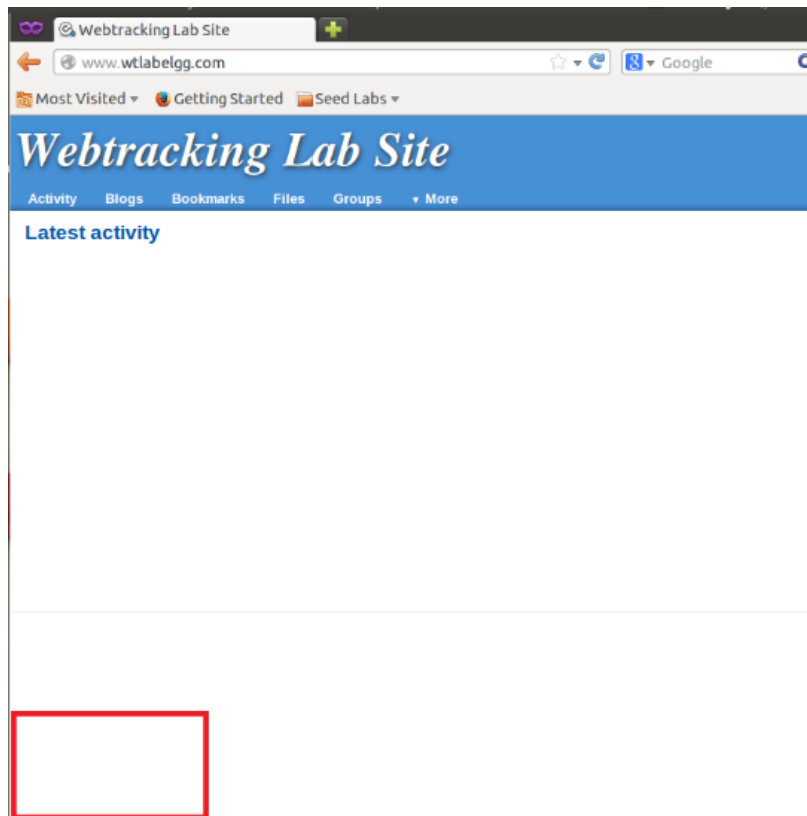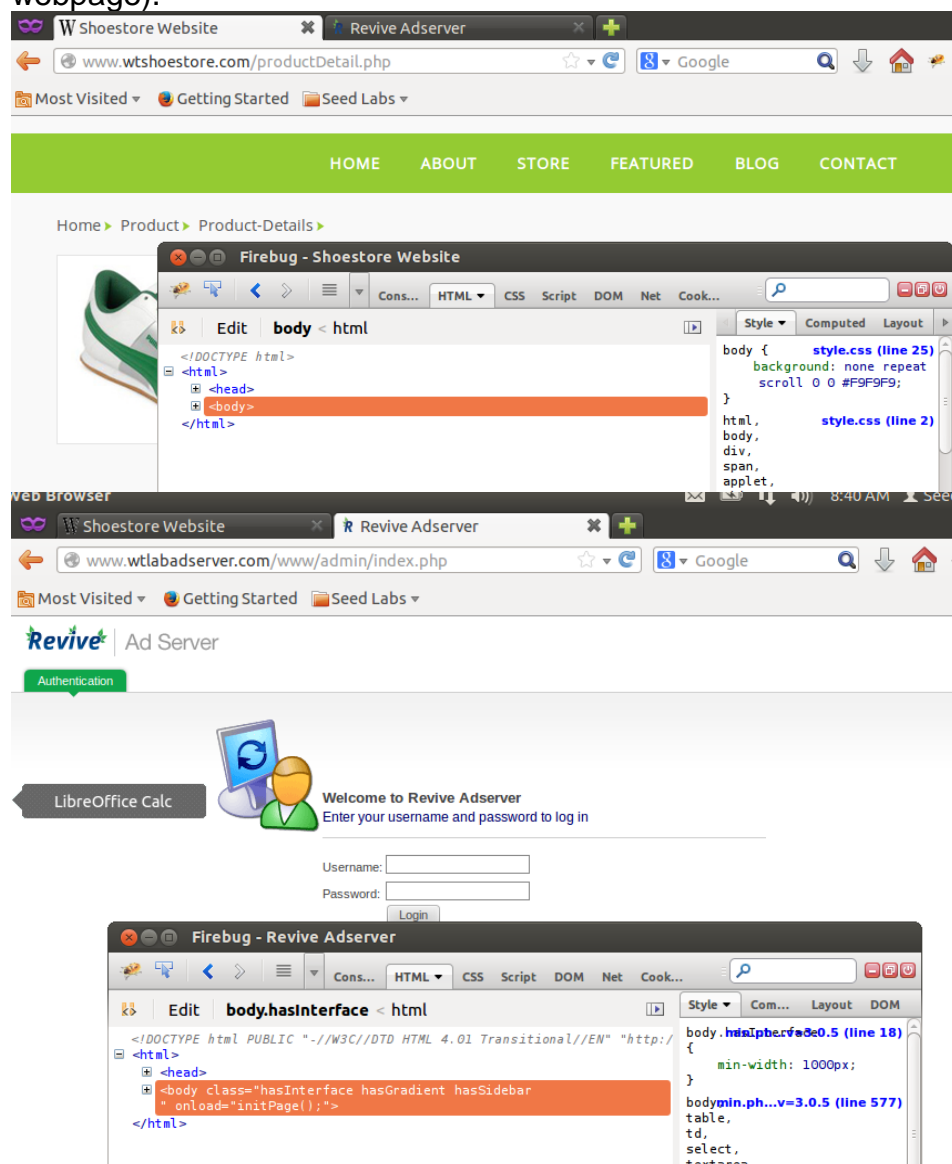 2. Click on view details for any product in the website.
  3. Open www.wtlabadserver.com/preferences.php in a new tab and observe the webpage.


Product Guid	Product	Category	Impression Count	UserTrackID
8678892570671441	Puma	Shoes	1	7705974851840588

In the preferences page, the recently visited documents are saved in a unique id allotted the user which is saved in the database for displaying the ad on other pages.

- **How ads are displayed in website**
  1. Open the Elgg website in Firefox browser.
  2. Capture and observe the LiveHTTPHeader traffic of the Elgg website, identify the HTTP requests which are from a different domain (third party).
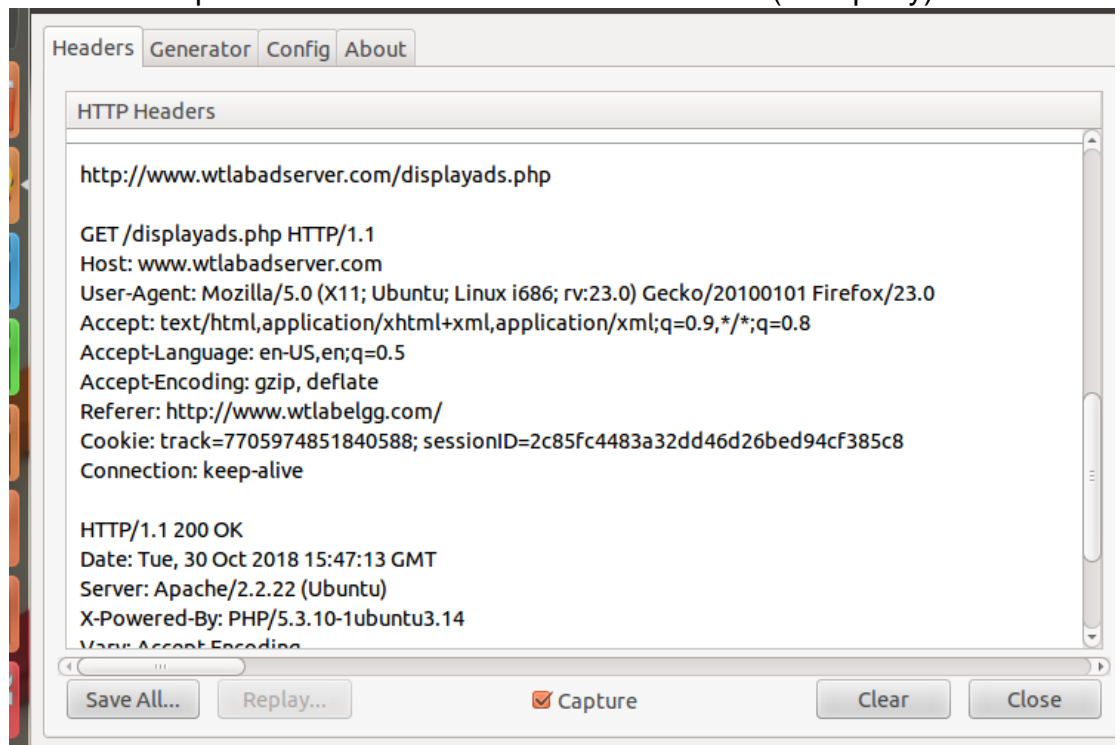

In the LiveHTTPHeaders, it's clearly observed how the display ads page has been requested. It searches for the cookies that that has been set recently and if there are any, they are displayed.

- **Tracking in a Private browser window**
  1. Open Elgg website without visiting any website and describe your observation in the lab report.
  2. Open Firefox and open the CameraStore, MobileStore, ElectronicStore and ShoeStore websites.

3. Click on view details for any products in the websites.
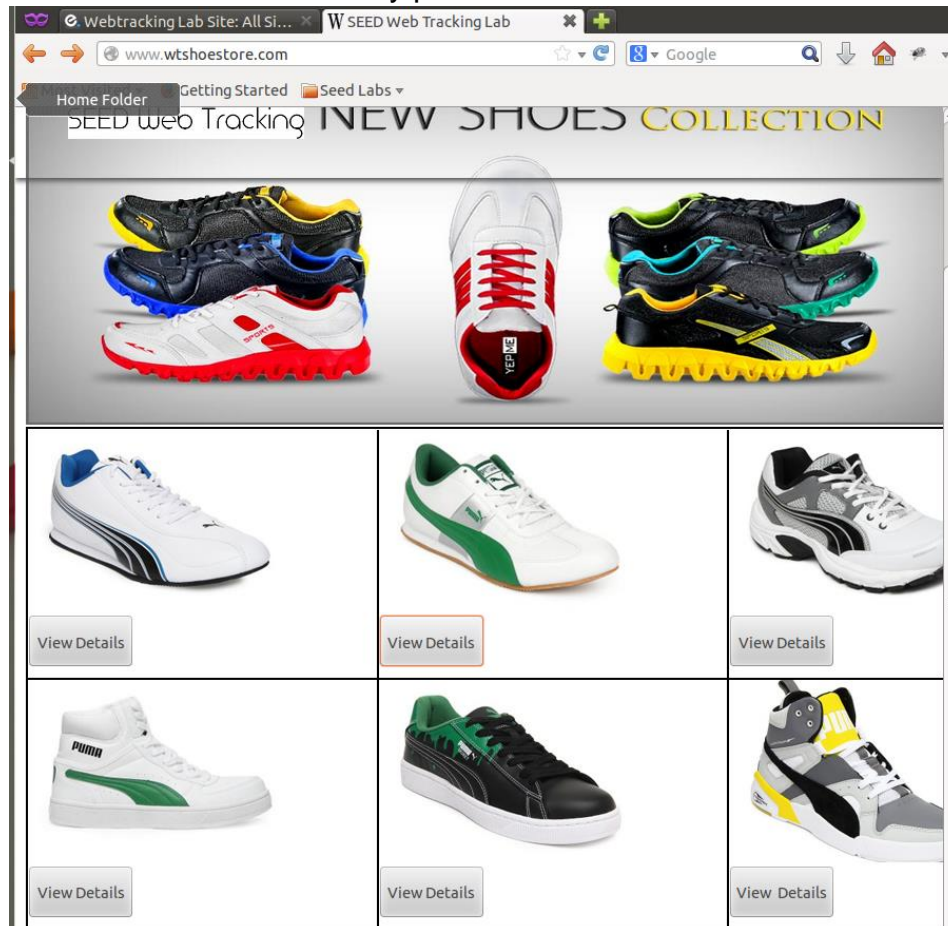
The sixth product was clicked three times and the other products were clicked only once.

4. Refresh the Elgg website in Firefox and describe your observation.
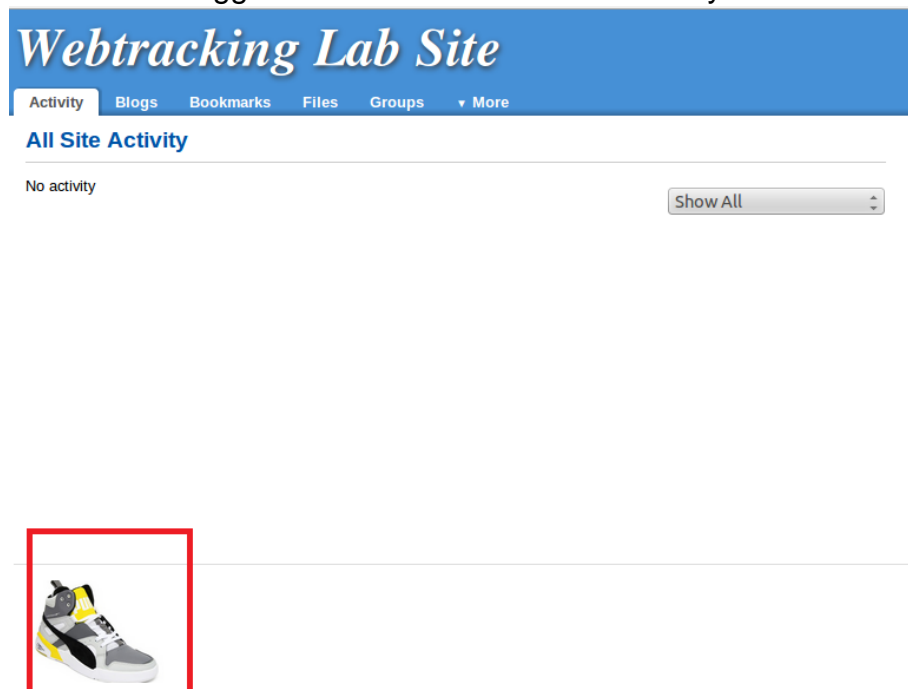
It was observed that refreshing the account which was signed in as a user, there was an ad displayed only of the product which was clicked multiple times.
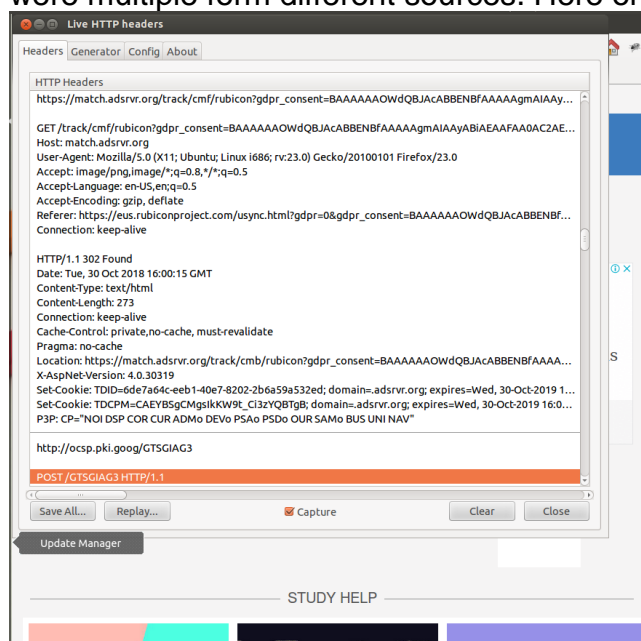
5. Close the InPrivate browser, reopen it and browse the Elgg website. Describe your observation.
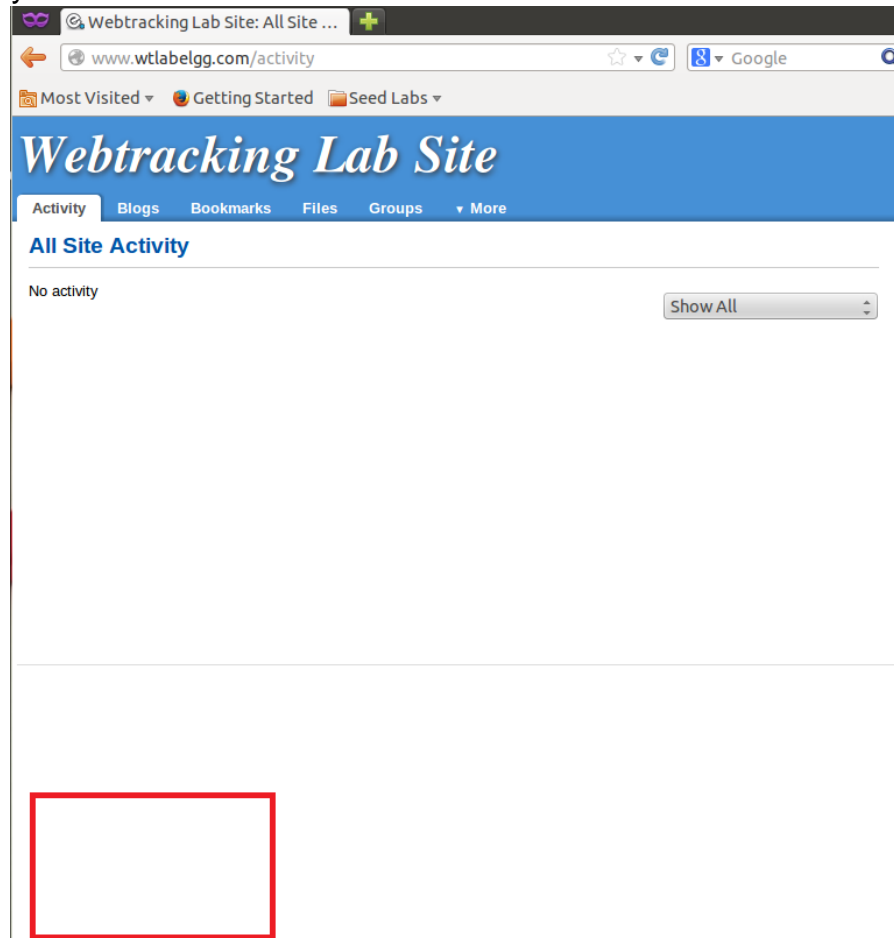
After closing and opening the browser again, the ad was not there.

- **Real World Tracking**
  For this task, http://dictionary.refernce.com was seen and the LiveHTTPHeaders were multiple form different sources. Here one of the example is shown


In this it is clearly seen that how the request has been made and is accepted and displayed on the screen.

- **Countermeasures**
  1. Disable the third party cookies from the Firefox browser. Please follow the instructions of how to disable third party cookies in Firefox browser in https://support.mozilla.org/en-US/kb/disable-third-party-cookies.
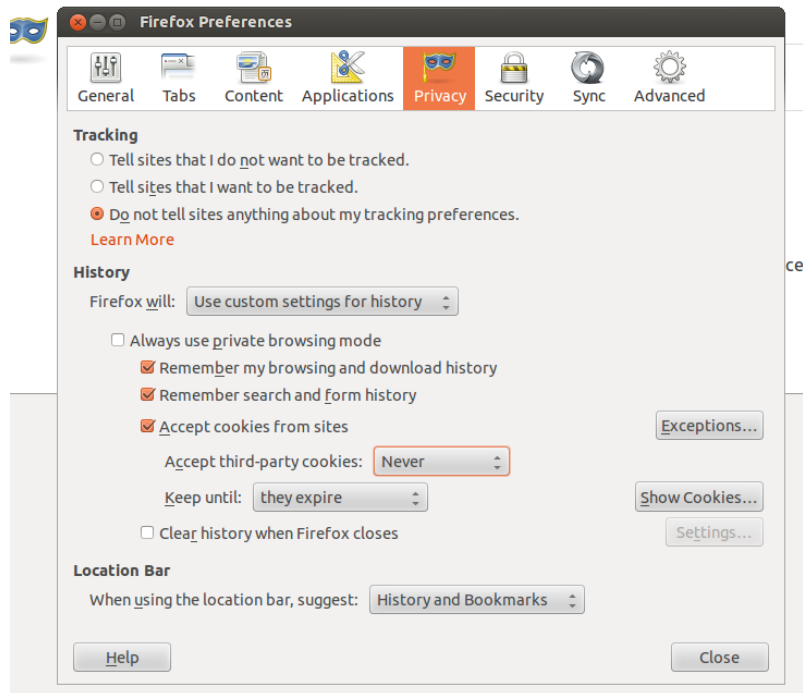

  2. After disabling the third party cookies, open the CameraStore, MobileStore, ElectronicStore, ShoeStore websites and LiveHTTPHeaders.
  3. Click on view details for any products in the websites.
  4. In LiveHTTPHeaders, identify the HTTP request, which set the third party cookies, and take the screenshot.
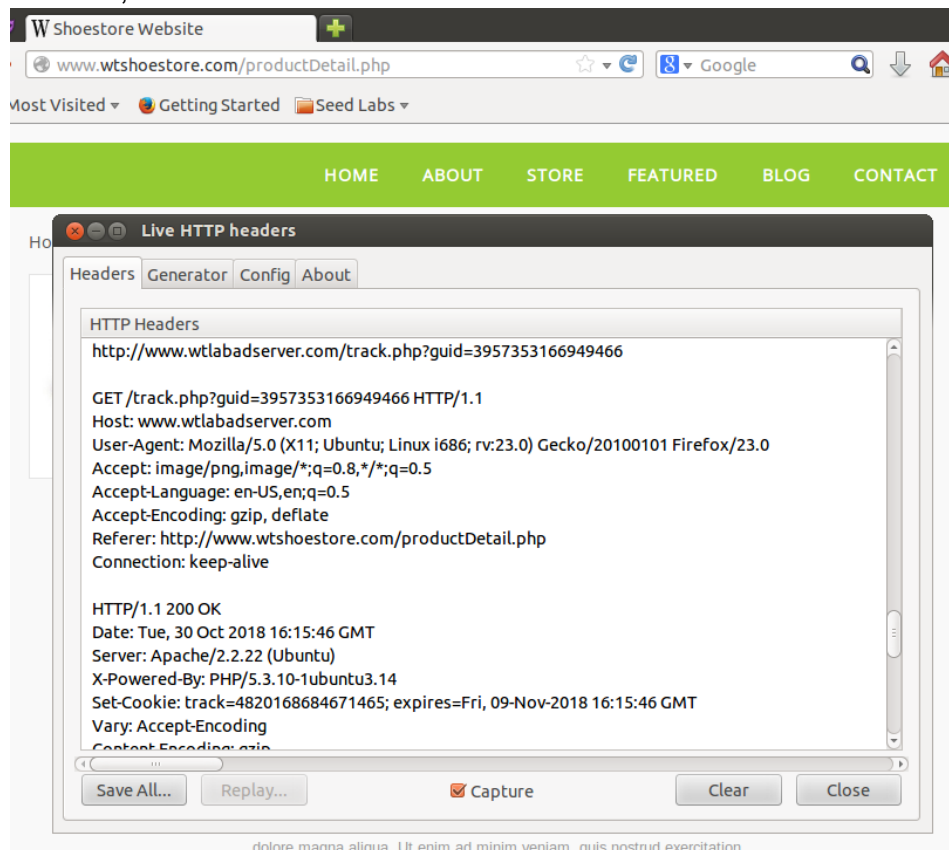
5. Open Elgg website and describe your observation. Also take the screenshot of HTTP request to ads server in LiveHTTPHeaders. Compare it with the HTTP request to ads server in Task 4 and explain the difference.
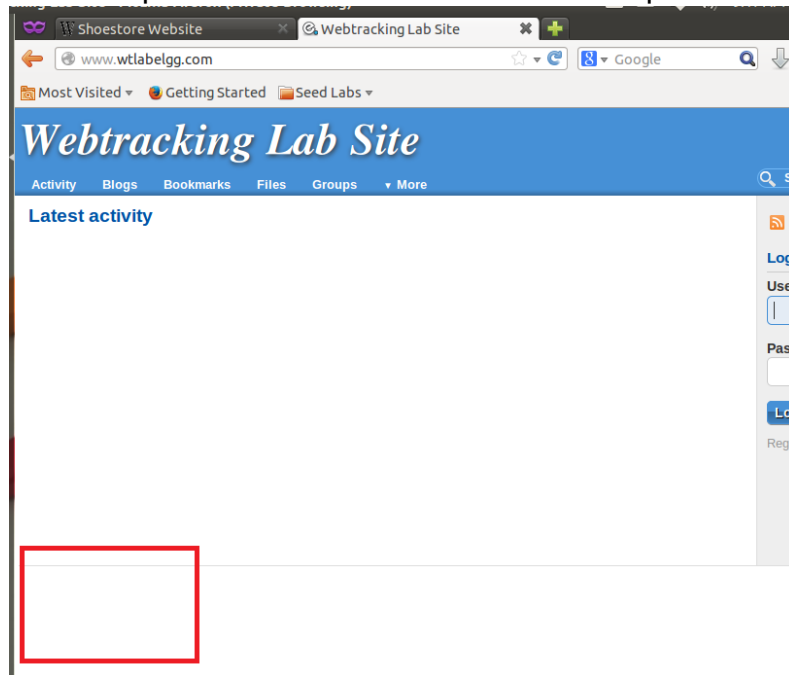
It has been observed now that there are no ads on the elgg site since the cookies are not been sent.
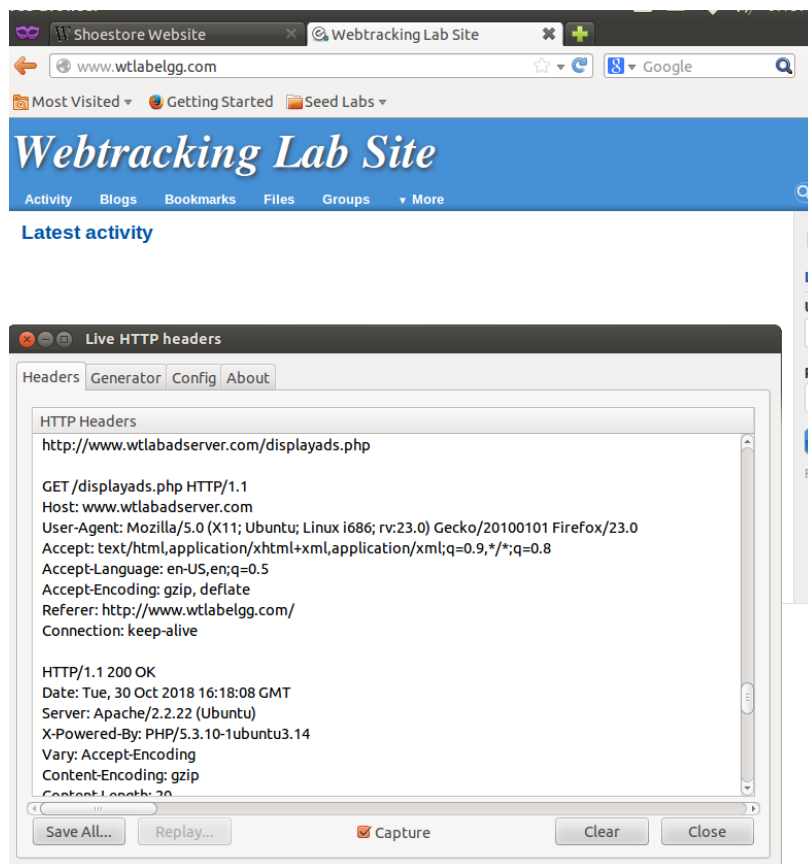
The cookies are not being generated so the ad server is also not getting.