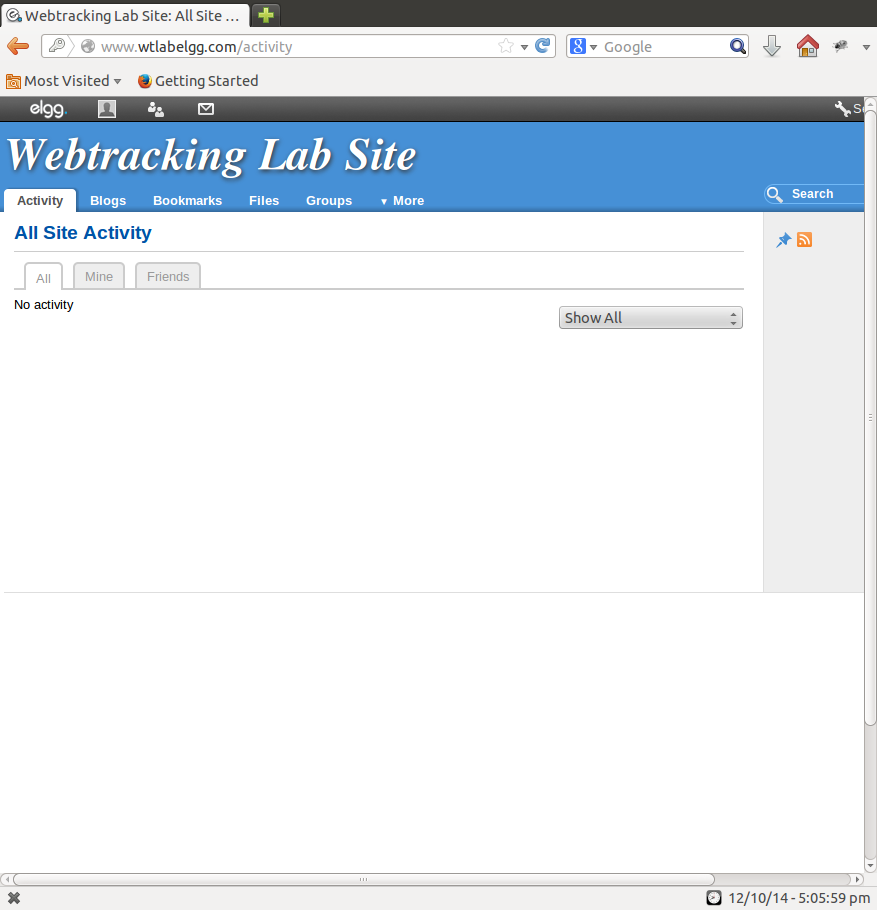
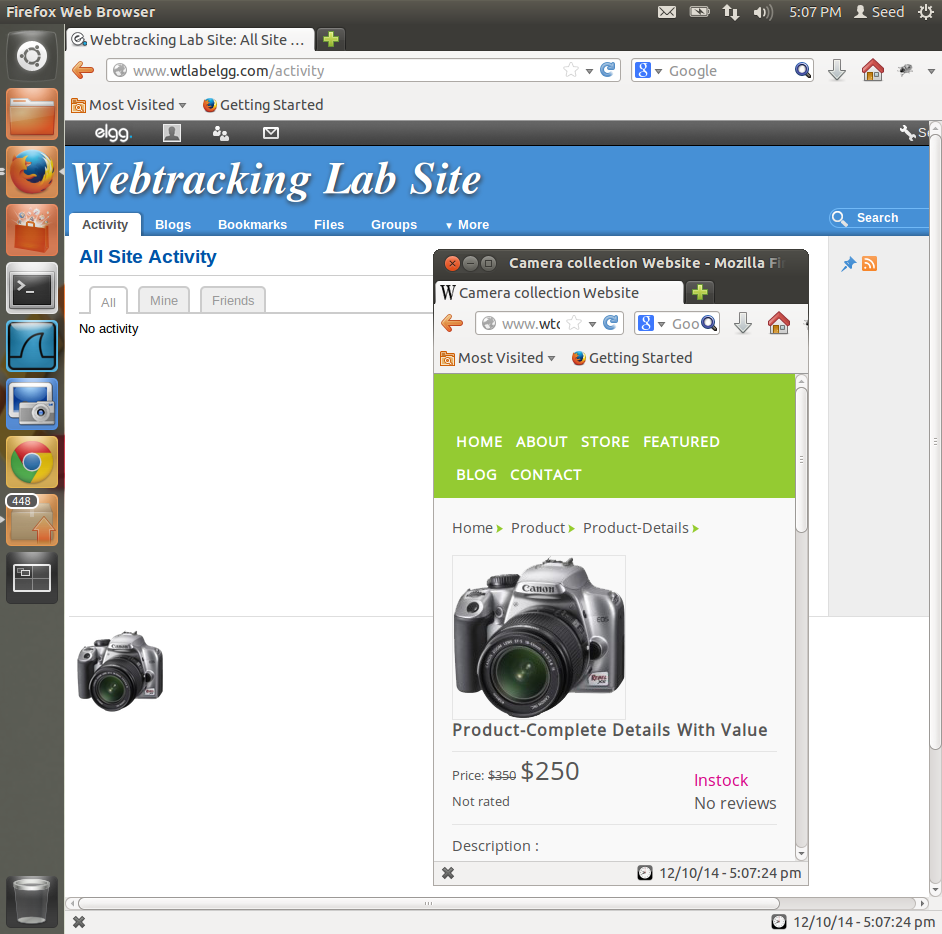
**Web Tracking Lab Report**

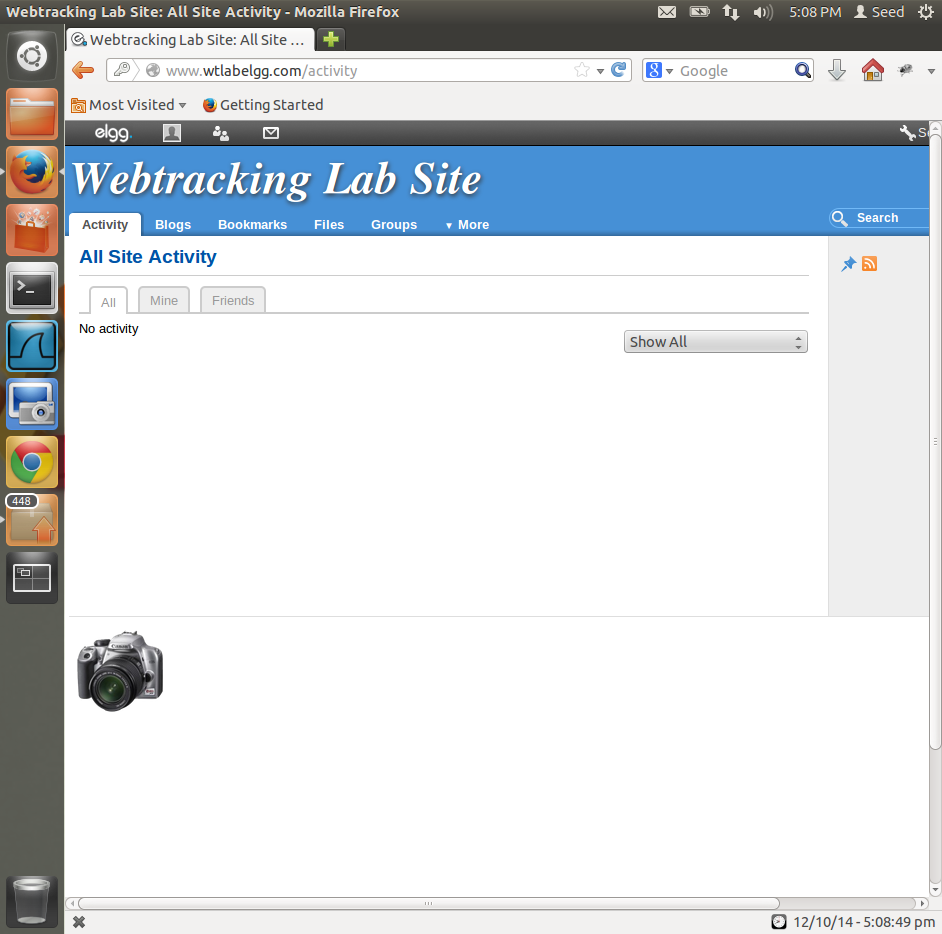
**Task 1:**

  
**Figure 1.1**

No ad displayed

 **Figure 1.2**

Ad displayed after visiting website



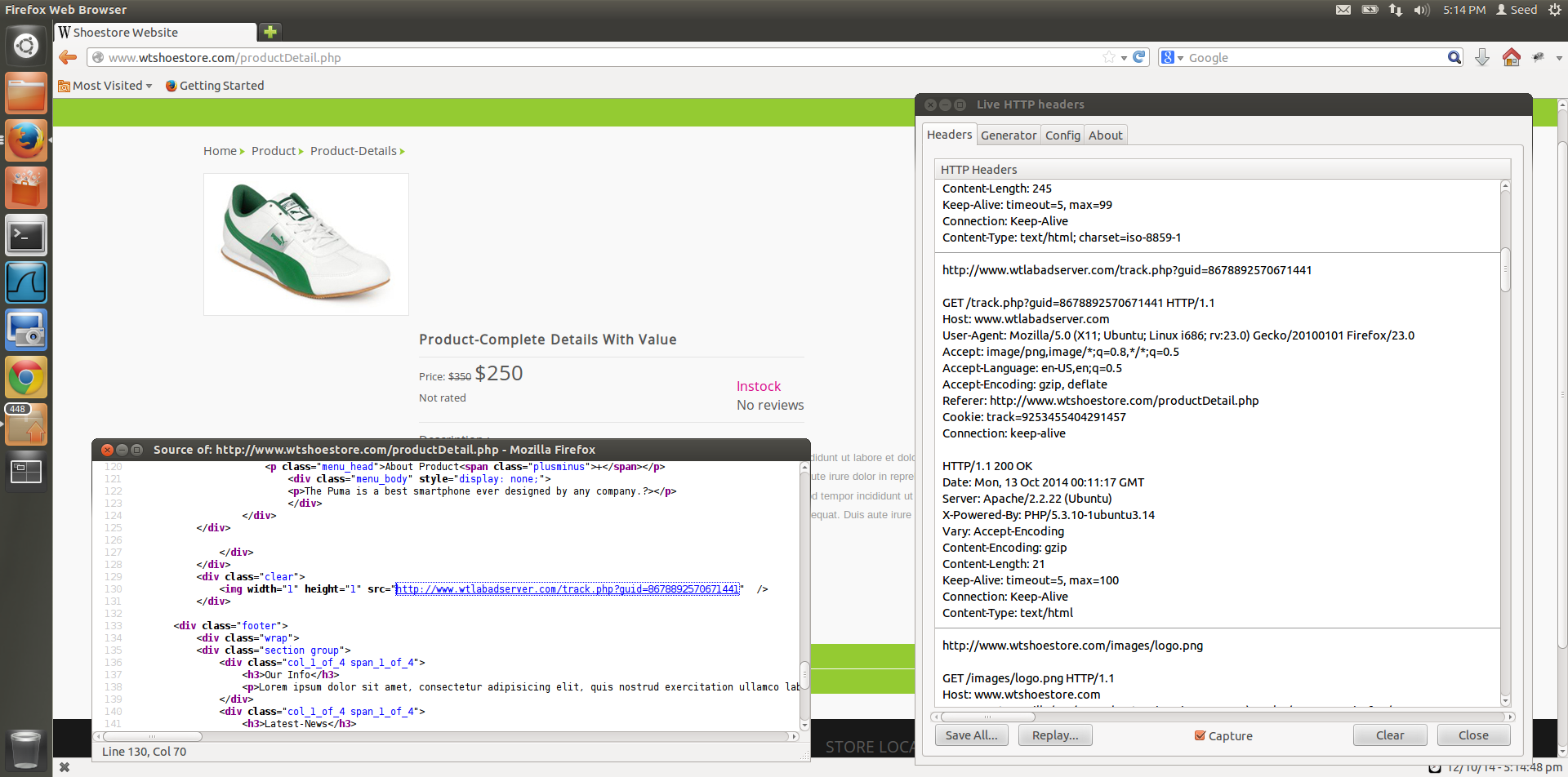
Ad persists even after reopening the elgg website

**Figure 1.3**

**Observations and Explanation:**

1. When Elgg is opened without visiting any ads, we see no ads being displayed in Figure 1.1, this because there is no history or cookies of any search made by the user.
2. After opening the various websites such as [www.wtcamerastore.com](http://www.wtcamerastore.com), [www.wtshoestore.com](http://www.wtshoestore.com) etc. and viewing the products and their details when we refresh elgg website we see the ads being displayed now with the product that was viewed most number of times (Figure 1.2).
3. On closing all the browsers and reopening them, we see that the ads are still being displayed in the elgg website, this shows that the user’s searches have been identified by the use of cookies being stored by the website on the browser (Figure 1.3).

**Task 2:**

****

Cookie used for tracking can be seen from LiveHTTPHeader

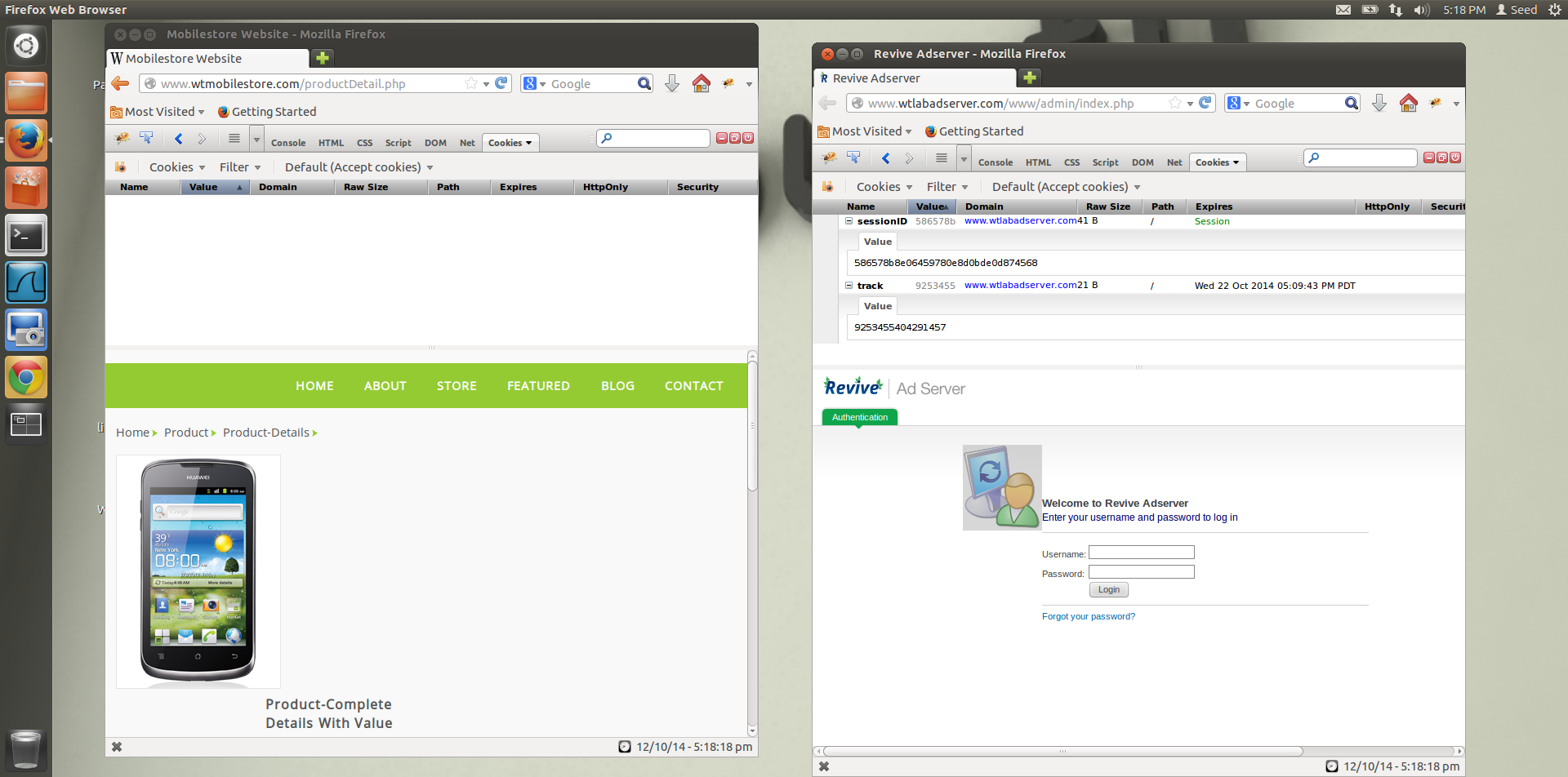
Request for tracking cookie from webpage

­­

**Figure 2.1**

**Observations and Explanation:**

1. LiveHTTPHeaders can be used to identify the tracking cookie in Firefox.
2. After opening the details of the product on the ShoeStore website, and using the LiveHTTPHeaders we can see that the cookie is set from wtlabadserver.com, this is a third-party cookie.
3. When we right click on the productDetails webpage and select the view page source option. We can see a div tag that contains the address of the site from where the image that sets the cookie is being fetched. By sending an image of width 1 and height 1 with src as the adserver website , request for tracking cookie is sent from the webpage
4. Third-party cookies are set by website with domain name other than the one the user is currently using, in our case, we are using the ShoeStore website and the third-party cookie is being set by [www.wtlabadserver.com](http://www.wtlabadserver.com)
5. Cookies are very important in web tracking as it allows the ad servers to set the cookies and display ads based on user preference, cookies allow the ad servers to store data about the user and his browsing habits, they store the user id, the product which the user has browsed and the number of times the user has viewed the product.



Firebug extension for wtlabadserver

Firebug extension for productDetails

**Figure 2.2**

**Observations and Explanation:**

1. Opened [www.wtmobilestore.com](http://www.wtmobilestore.com) and visited product details.
2. Opened the [www.wtlabadserver.com](http://www.wtlabadserver.com) website
3. Opened the Firefox extension Firebug.
4. The Firebug extension on the adserver webpage showed 2 cookies. The sessions cookie and the third-party *track* cookie, which was generated by [www.wtlabadserver.com](http://www.wtlabadserver.com) when user viewed the mobile on the mobilestore productDetails page.
5. The third party cookie used in tracking the users search is the **track** cookie, as can be seen in the firebug extension used with the ad server webpage, the other cookie is the sessionID cookie which is used till the session lasts.
6. **Why is it called third party cookie?**

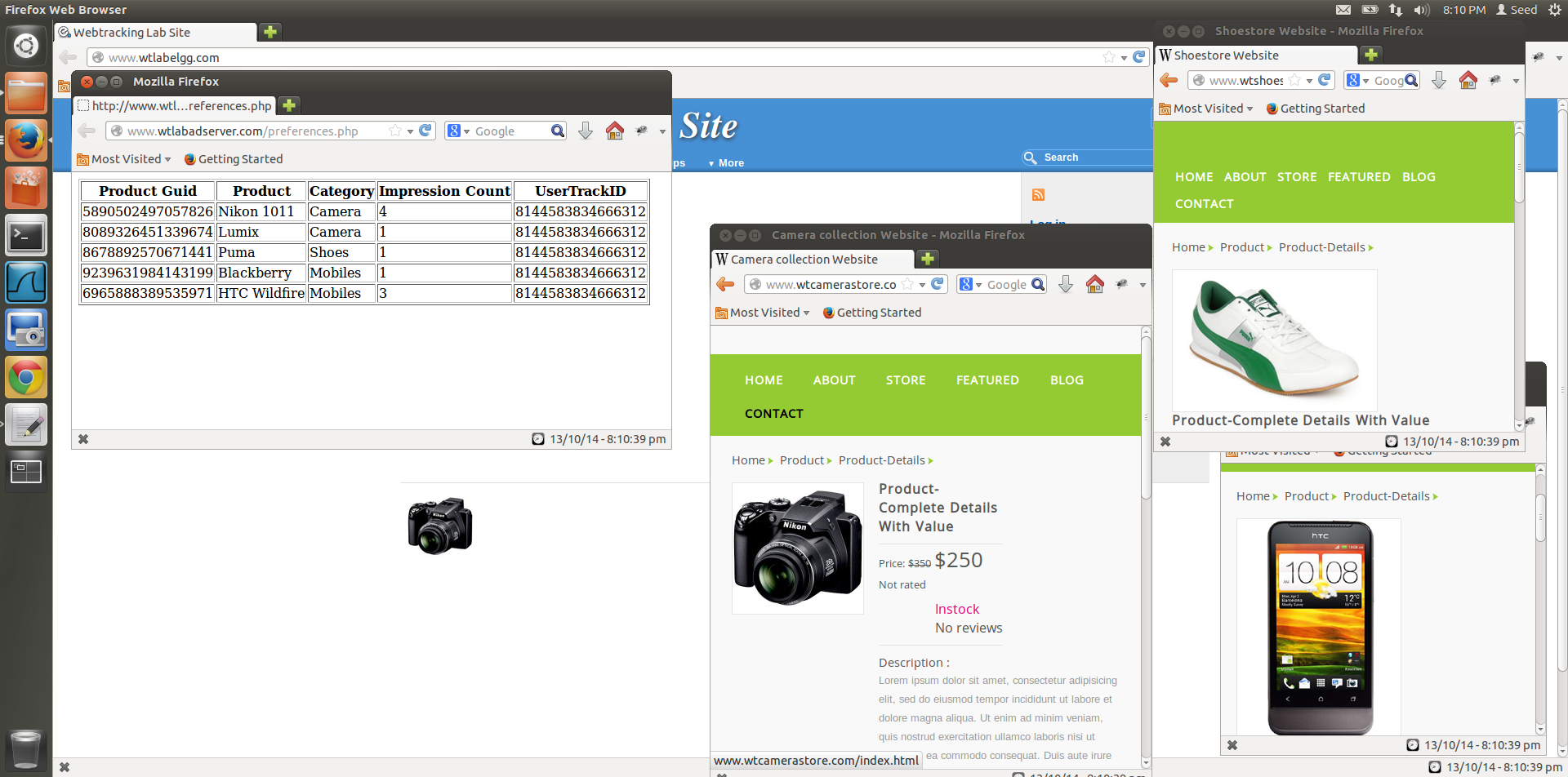
The mobile store, shoe store, electronic store and camera store contains images or other components stored on servers in other domains. Cookies that are set during the retrieval of these components are called as third-party cookies.

Third-party cookies are cookies that are set by website with a domain name other than the domain the user is currently using.

For example, user visits website example.com, which has an image that needs to be fetched from example2.com. This image request can set cookie on domain example2.com, and the cookie set on example2.com is known as a third-party cookie.

Third-party cookies are used for web tracking purposes and are used actively by ad servers to display relevant ads to the user.

**Task 3:**

****

Ad server web tracking

Each product has separate id

Number of times a product is viewed

Product with most impression Count is displayed in the ad on [www.wtlabelgg.com](http://www.wtlabelgg.com). Here Nikon 1011has 4 impressions (highest)

**Figure 3.1**

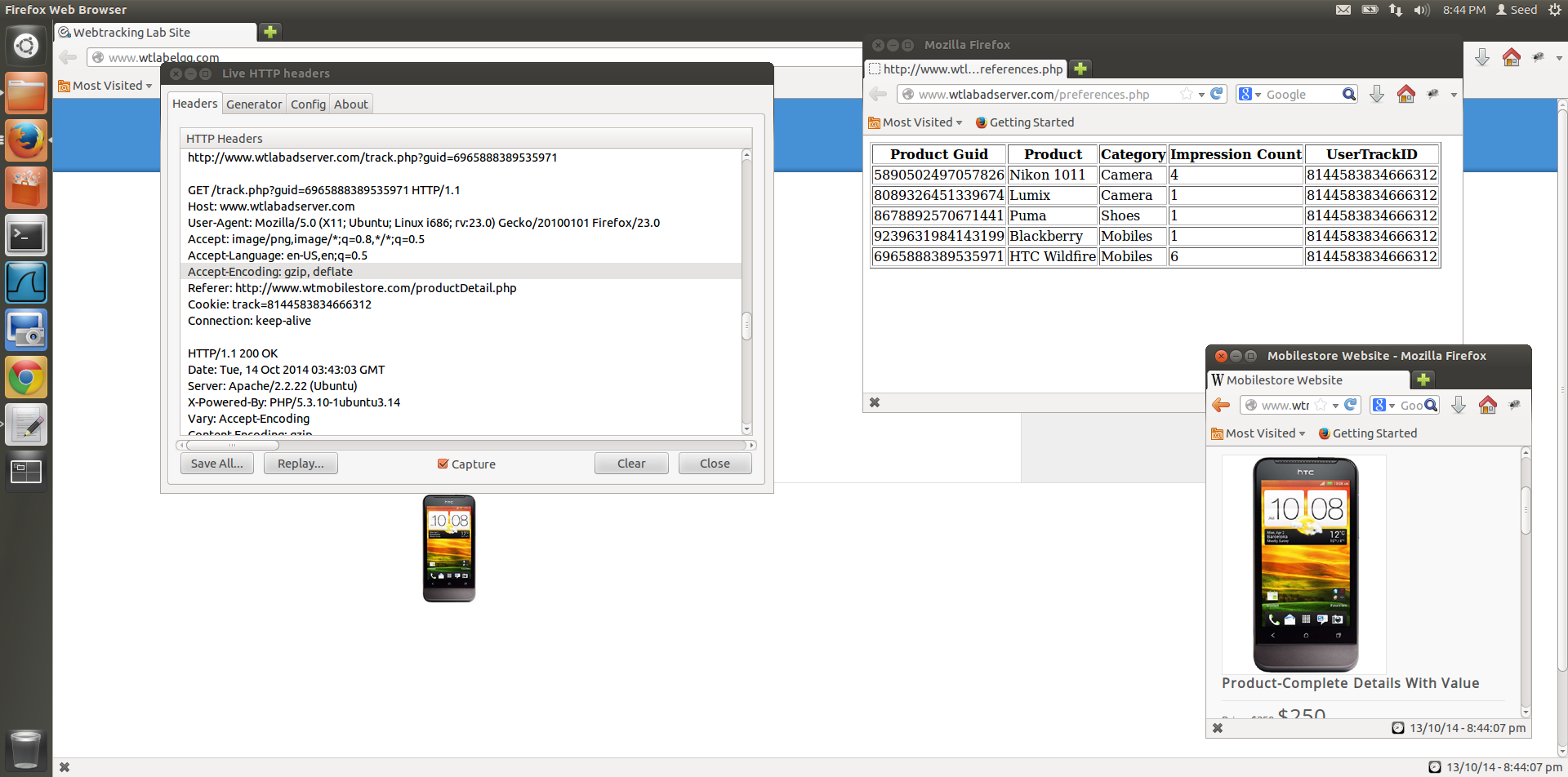
****

User id to identify where the request is coming from

Product with most impression Count is displayed in the ad on [www.wtlabelgg.com](http://www.wtlabelgg.com). Here HTC Wildfire has 5 impressions (highest)

Ad server web tracking

**Figure 3.2**

****

The user track id is sent with the track cookie value to see which user is being tracked.

Guid is sent in the header to tell the ad server which product is viewed

**Figure 3.3**

**Observations and Explanation:**

**How user impressions are logged in ad server database and how it is mapped to a user, give evidence to support your answer.**

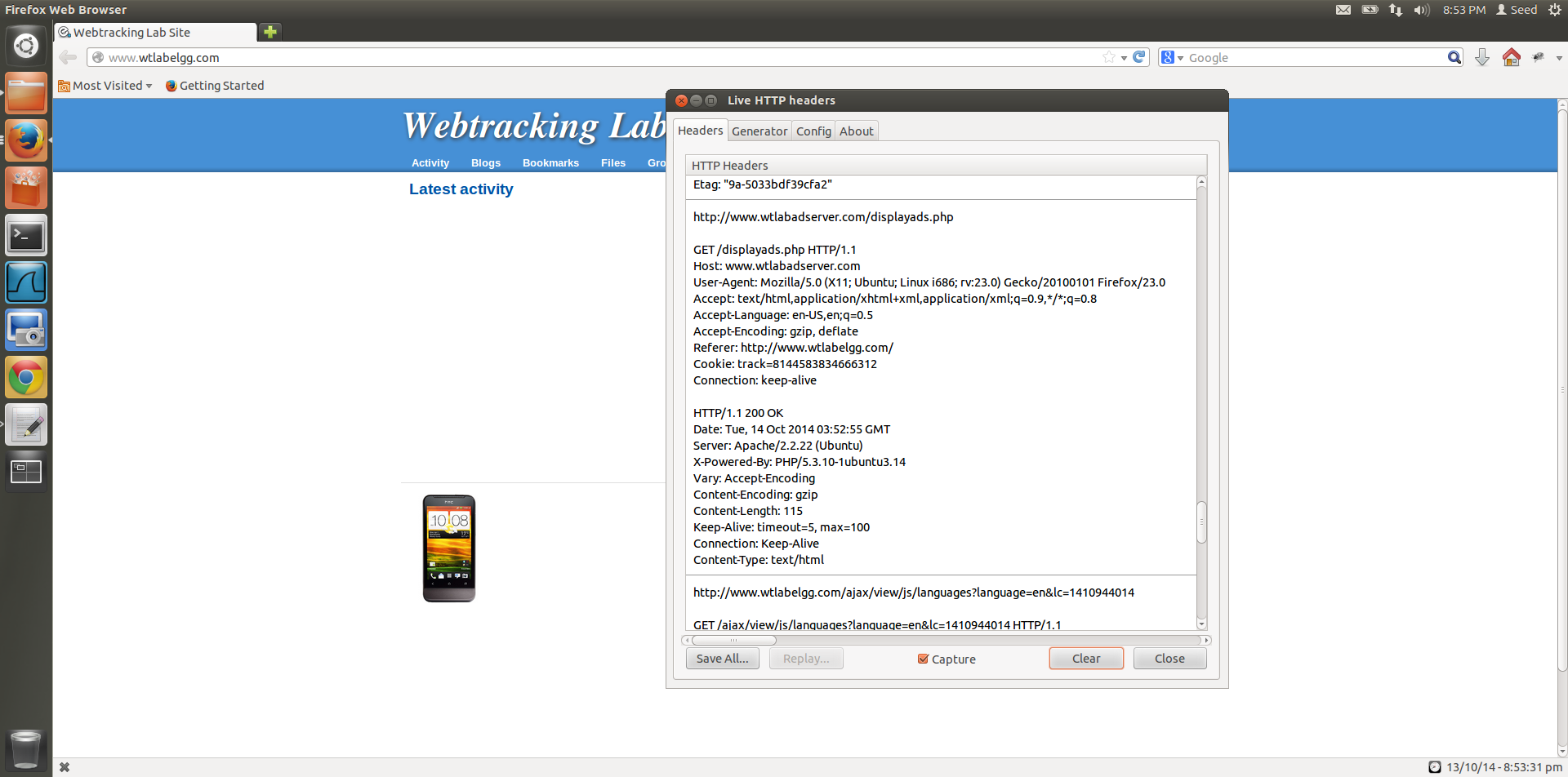
When we use an e-commerce website and view the product details of a website, the webpage that displays the details also has a web bug or beacon, to track user preferences, in the form of 1px by 1px image tag. So whenever we use the webpage, a request is sent to the third-party website (in our case [www.wtlabadserver.com](http://www.wtlabadserver.com)), to fetch this image from the webpage that has the information.   
Example of an embedded img tag that is from a third-party website inside the page source of the product website.

***<div class="clear">***

***<img width="1" height="1" src="http://www.wtlabadserver.com/track.php?guid=5890502497057826" />***

***</div>***

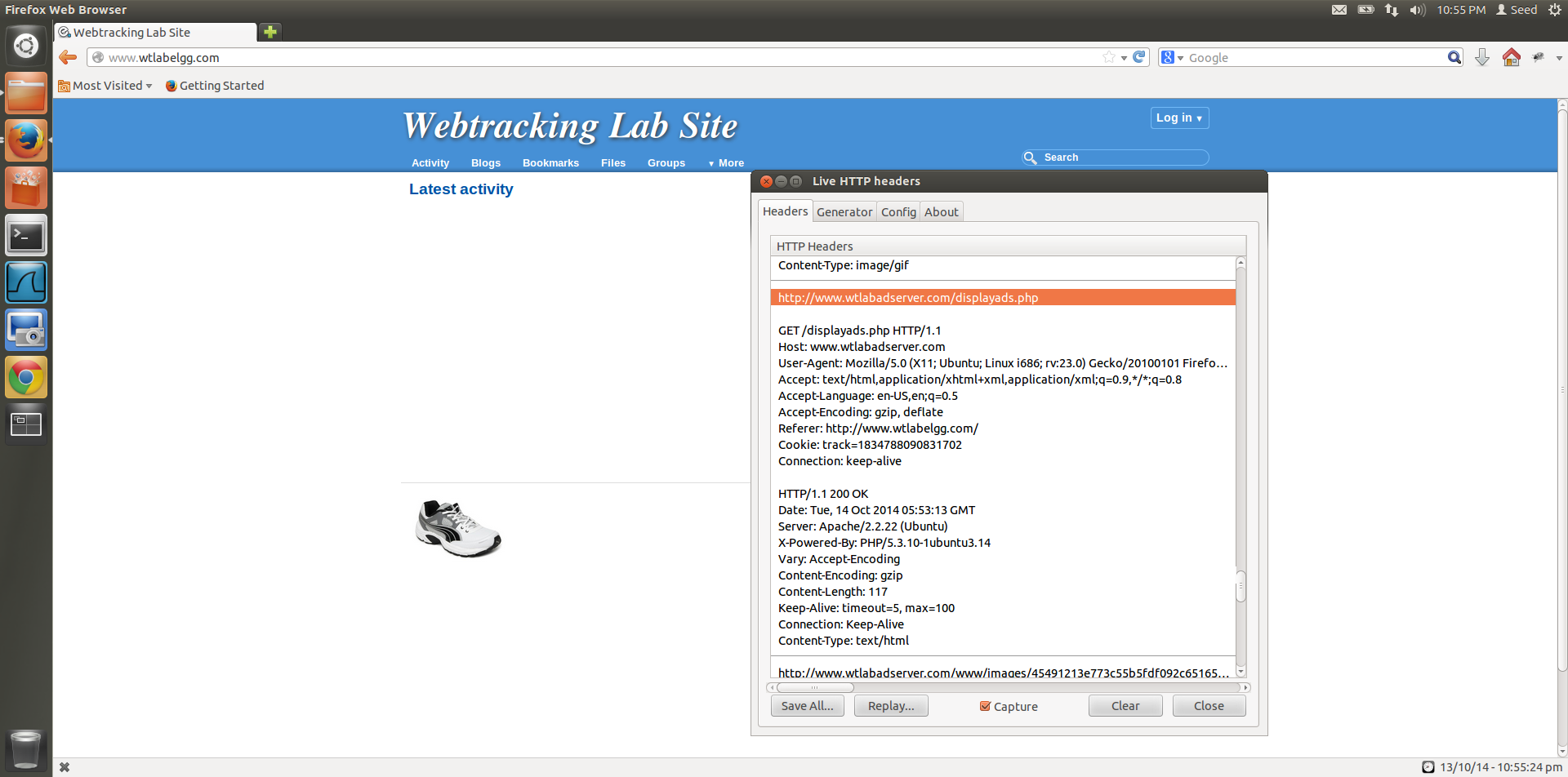
The USER TRACK id is sent in the header (Figure 3.3) to track the user and the guid is sent to track the product that is being used by this particular user, so every time the user opens this webpage the same cookie name=value pair is sent to the ad server, and the HTTP request header also has the guid of the product being viewed, with the help of this guid the impressions count is updated, each time the ad server receives a new request for the same guid. And when the ad server has to display ads, it receives the user track id in the request header from the elgg website and then displays the ad of the product that has the highest impressions count, in case 2 or more products have the same impresions count then the product that was viewed first is displayed.

**  
Figure 3.4**

The user track id is sent with the track cookie value to see which user is being tracked.

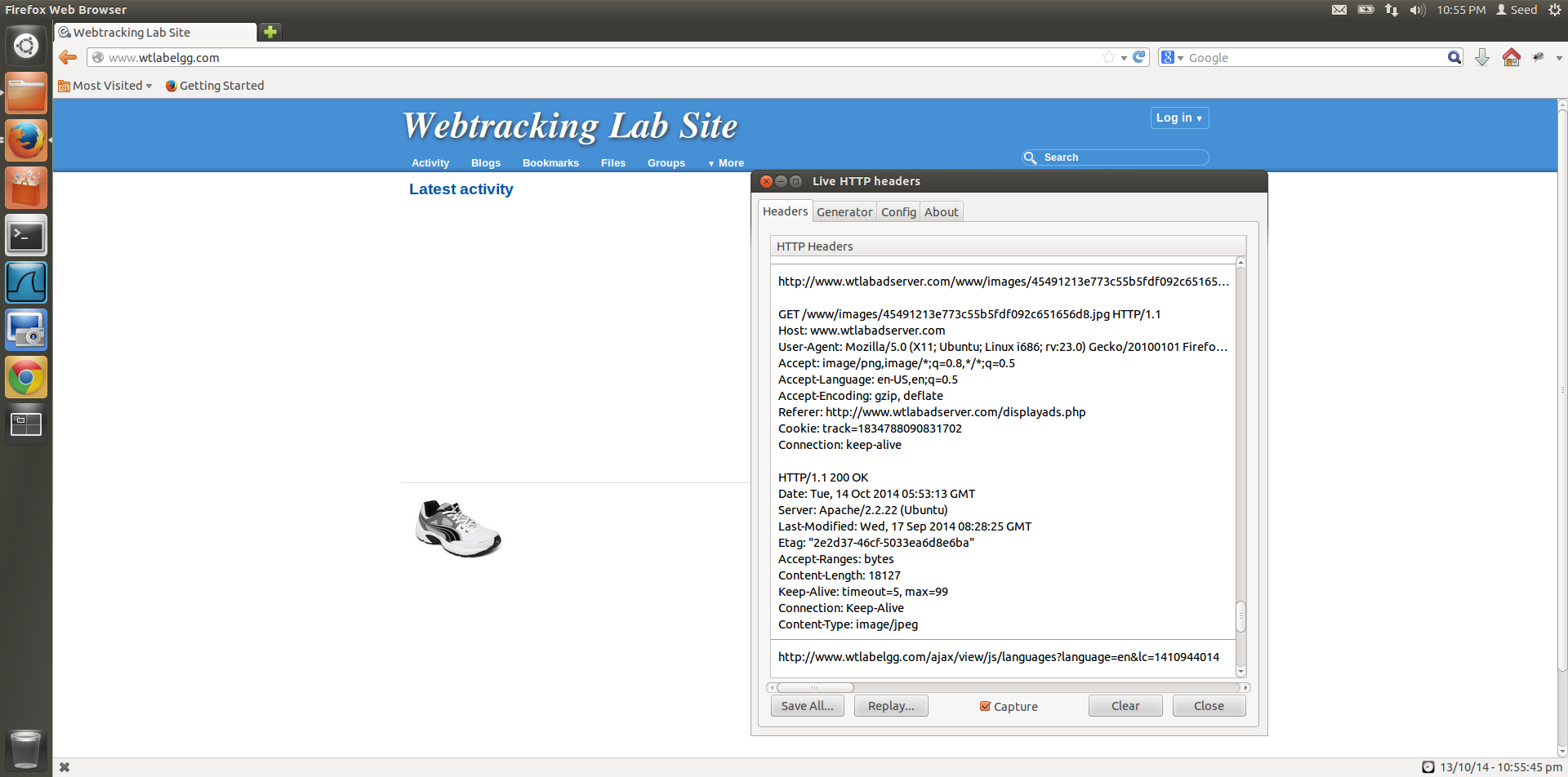
HTTP request from elgg, that displays the ads fetched from [www.wtlabadserver.com](http://www.wtlabadserver.com)

**Task 4:**

****

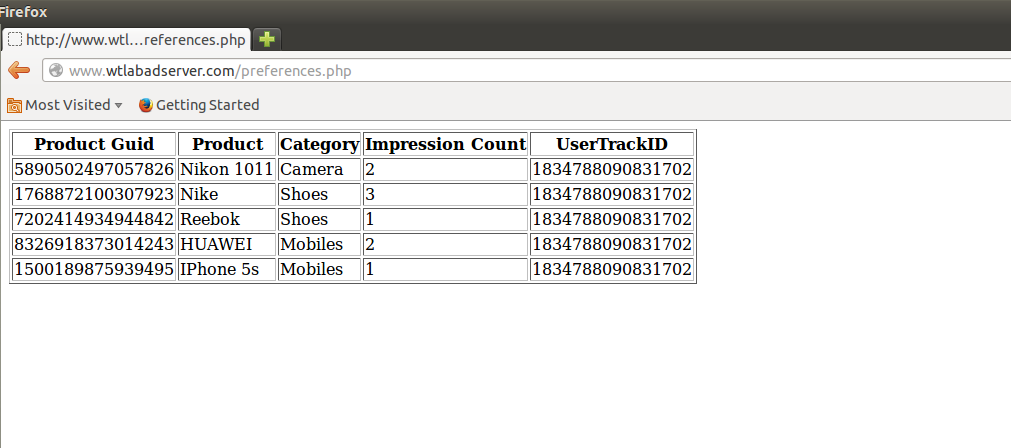
HTTP request from ad server to display the ad based on users history

**Figure 4.1**

****

HTTP request to get the image that has to be displayed on elgg website

**Figure 4.2**

****

User id identifies the person that is viewing the products on e-commerce website

Number of times the user has viewed this product

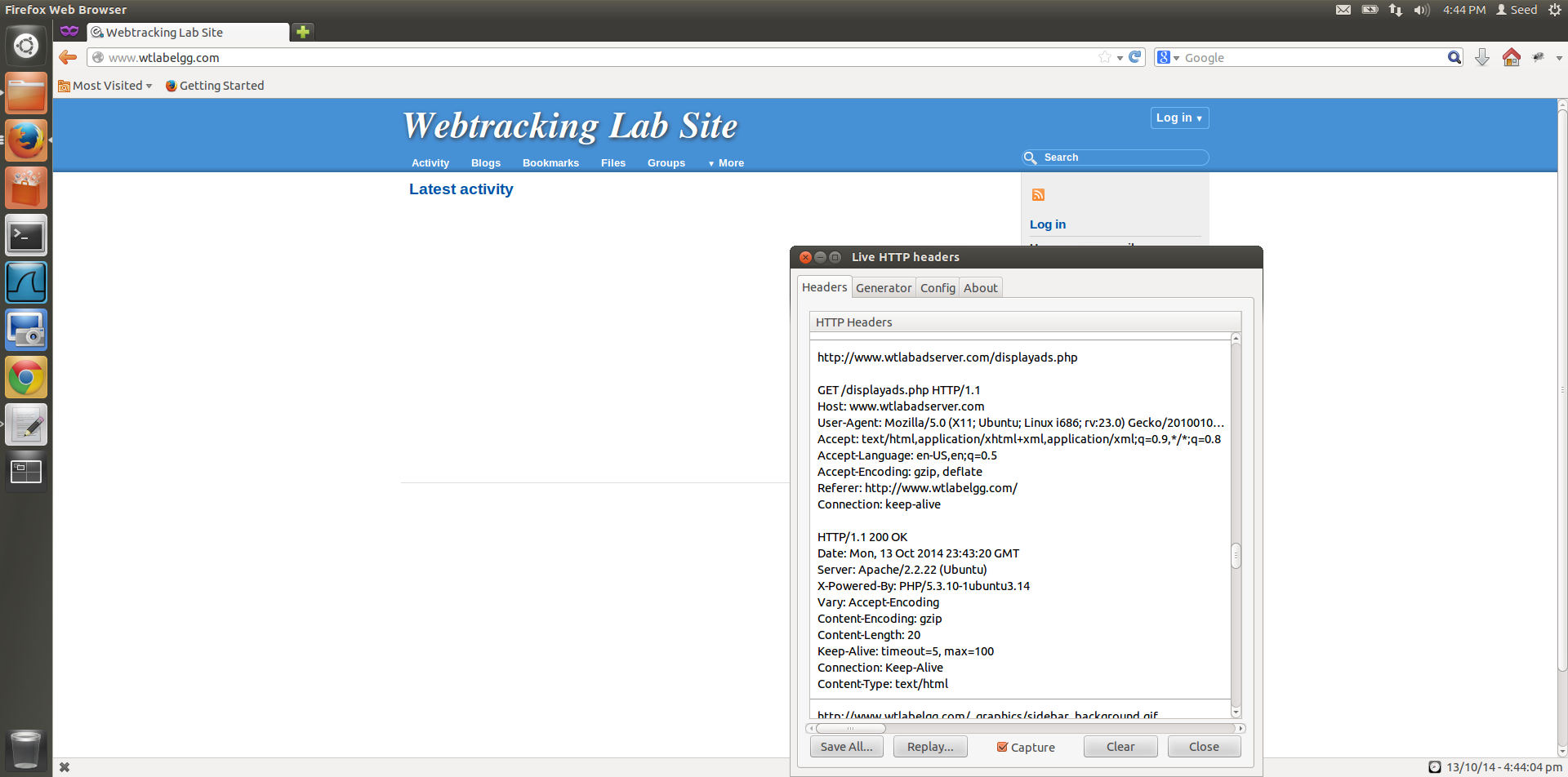
Product id to determine which product user is interested in and to show ads accordingly

**Figure 4.3**

**Observations and Explanation:**

1. The request header in Figure 4.1 is to the [www.wtlabadserver.com/displayads.php](http://www.wtlabadserver.com/displayads.php) website to display ads on elgg website. This request header contains he cookie track value and the referrer website, which tells the ad server that the request is coming from elgg.
2. The request header in Figure 4.2 is coming from [www.wtlabadserver.com/displayads.php](http://www.wtlabadserver.com/displayads.php) this request is getting the image for the ad that must be displayed on elgg website, it contains the track value of the user who is accessing elgg, this allows for targeted ads to be displayed to the user, as only dependent on his search and cookies, are the ads displayed. These user interests are maintained by storing the user id as a cookie and then accessing the cookie to display relevant ads, the user id obtained from the cookie allows for the ad server to fetch the product which the user has viewed most number of times by referring to the impressions count field and then using the product guid to fetch the image that has to be displayed in the ad, and display it on elgg website.
3. Figure 4.3 shows the table that is maintained by the ad server to display the targeted ads to the user. The various pages have been visited and the page that has been visited the most is the Nike shoe page and that has been displayed as the ad on the elgg webpage.

**Task 5:**

****

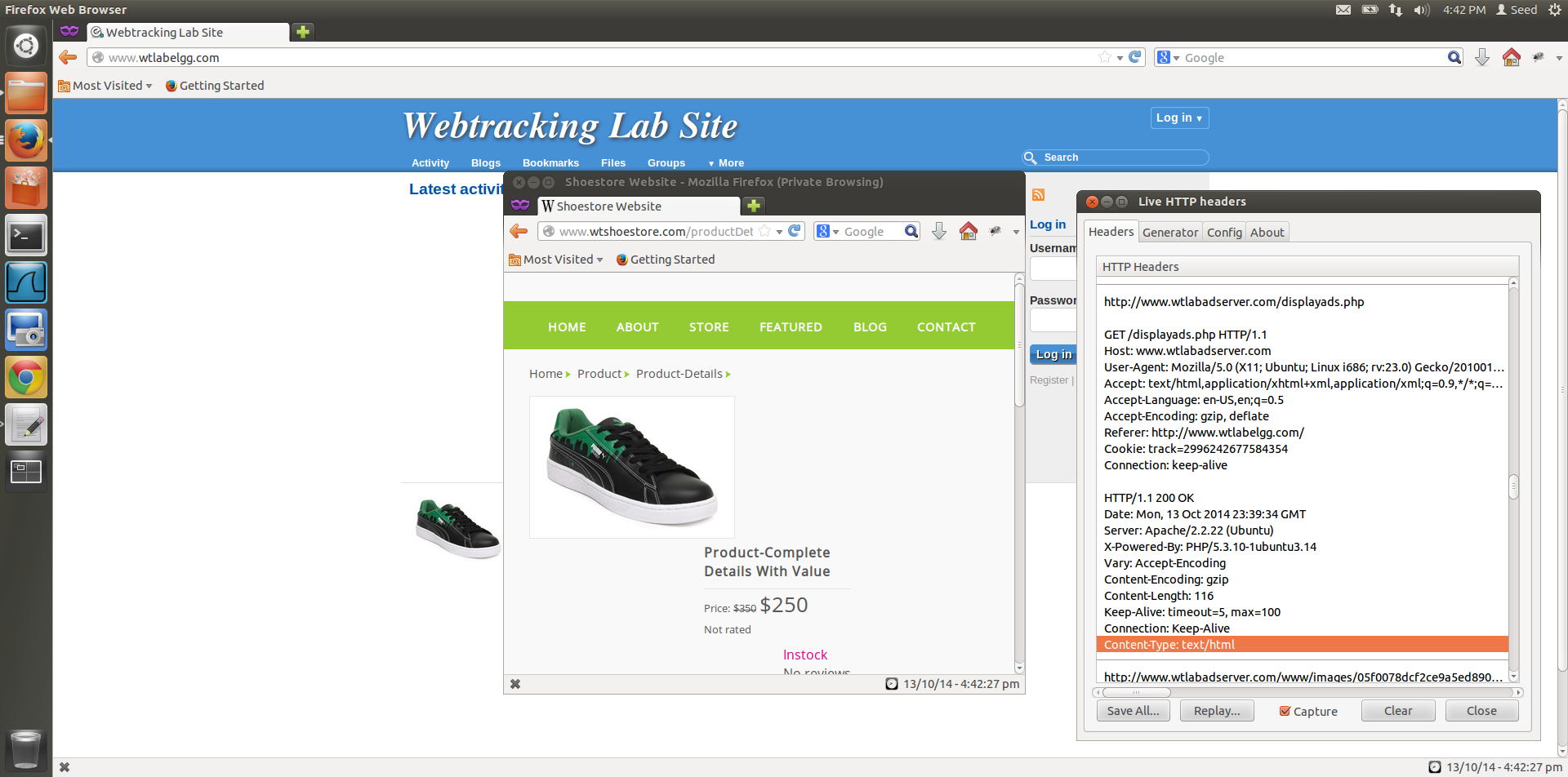
Request Header from third part website to display ad (wtlabadserver.com) but cookies do not exist due to new private browsing window

No cookie as this is a new private browsing session, so no previous browsing history exists

No ad displayed, new Private browsing window, so no cookies from previous browsing

Private browsing

**Figure 5.1**

****

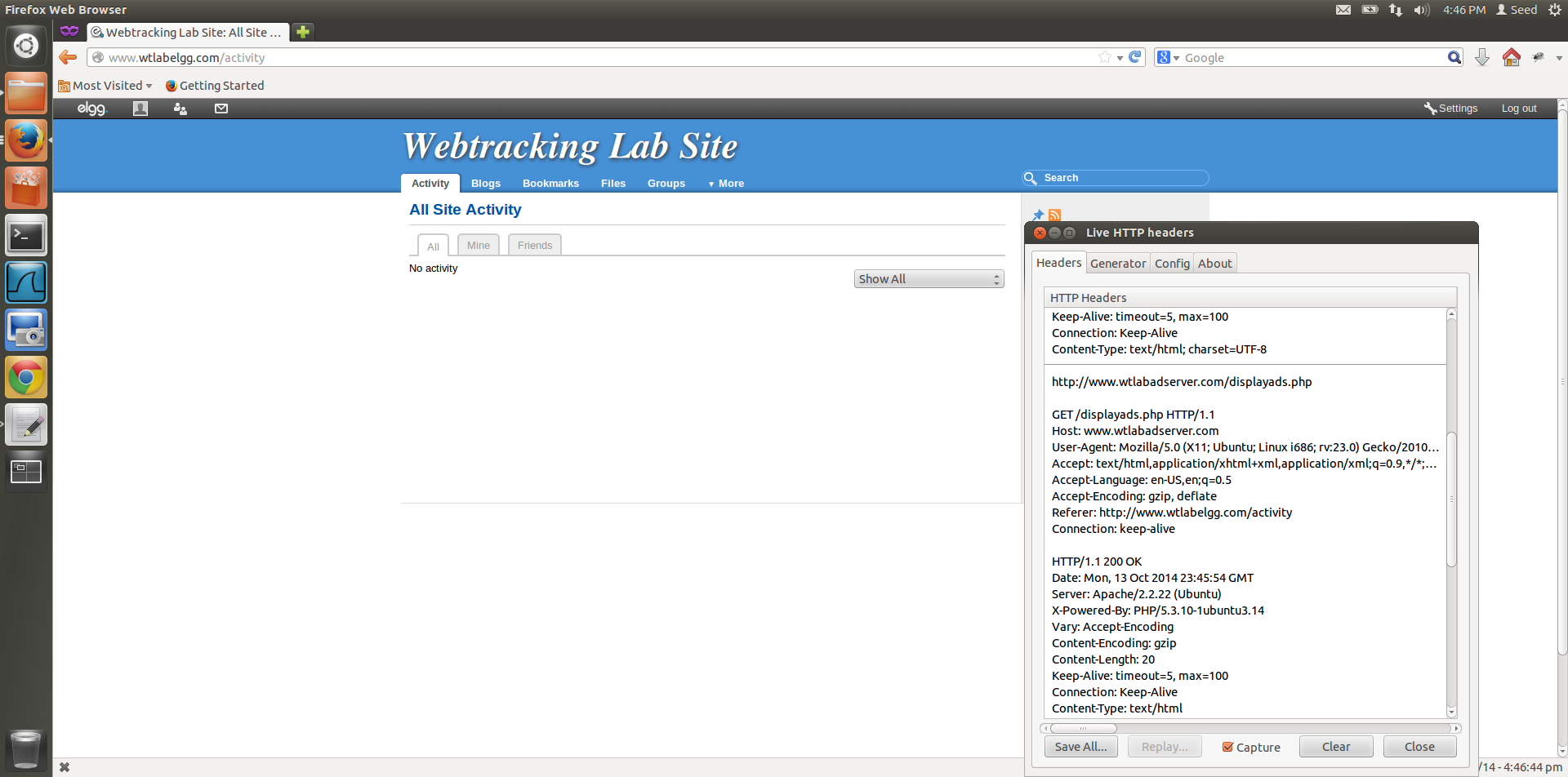
HTTP request to ad server from private browsing window

Third party cookie used for request

Private browsing of e-commerce website, stores cookie

Ad displayed, as cookies are stored for Private browsing as well, but only till the window is open

**Figure 5.2**

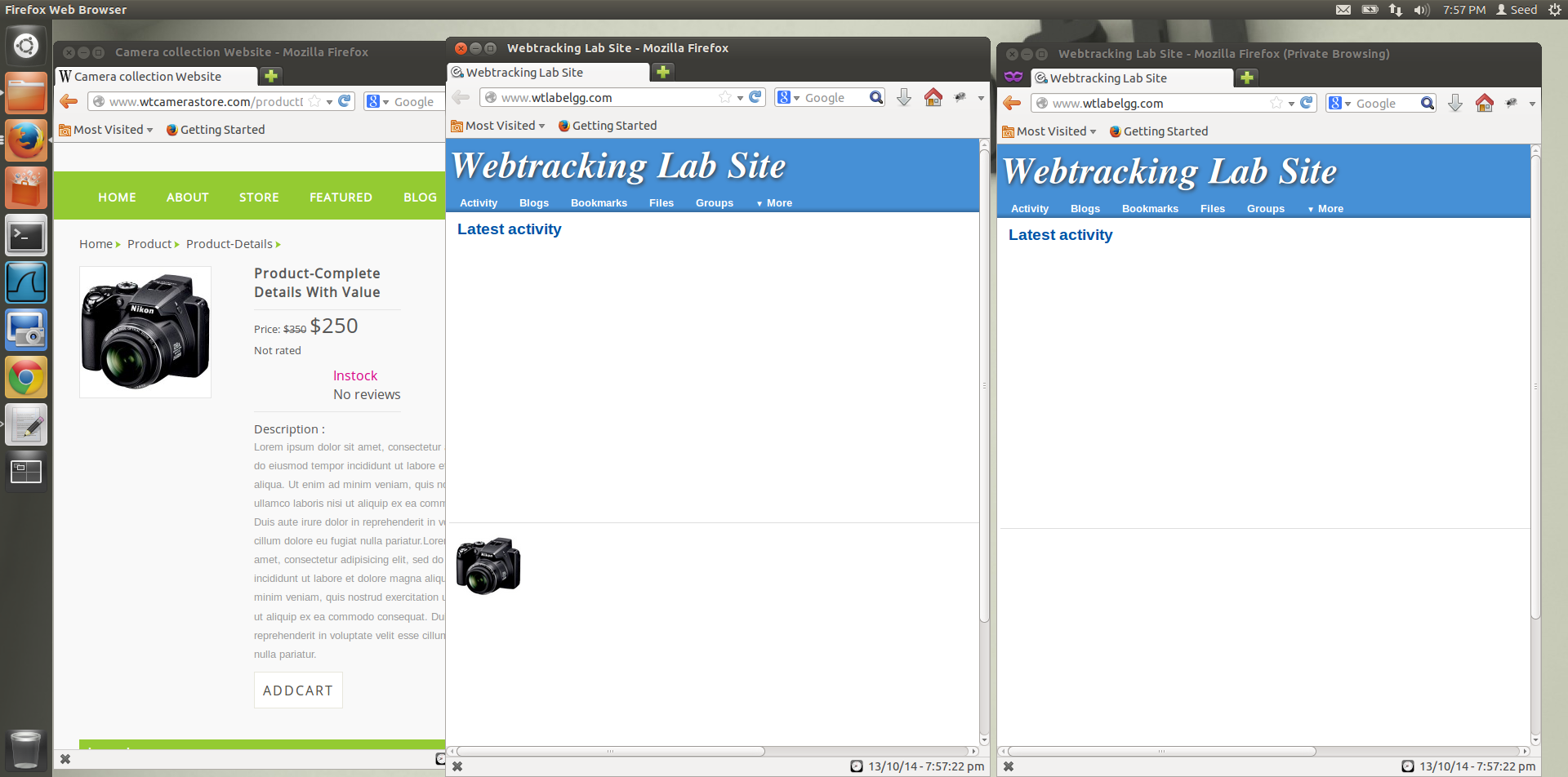
****

No ad displayed, new Private browsing window, so no cookies from previous browsing

Request Header for third part website (wtlabadserver.com) from the private browsing window

No cookie, as the previous private browsing cookies were discarded when the browser was closed

**Figure 5.3**

****

Private browsing of www.wtlabelgg.com and e-commerce websites

Private browsing window, ad not displayed

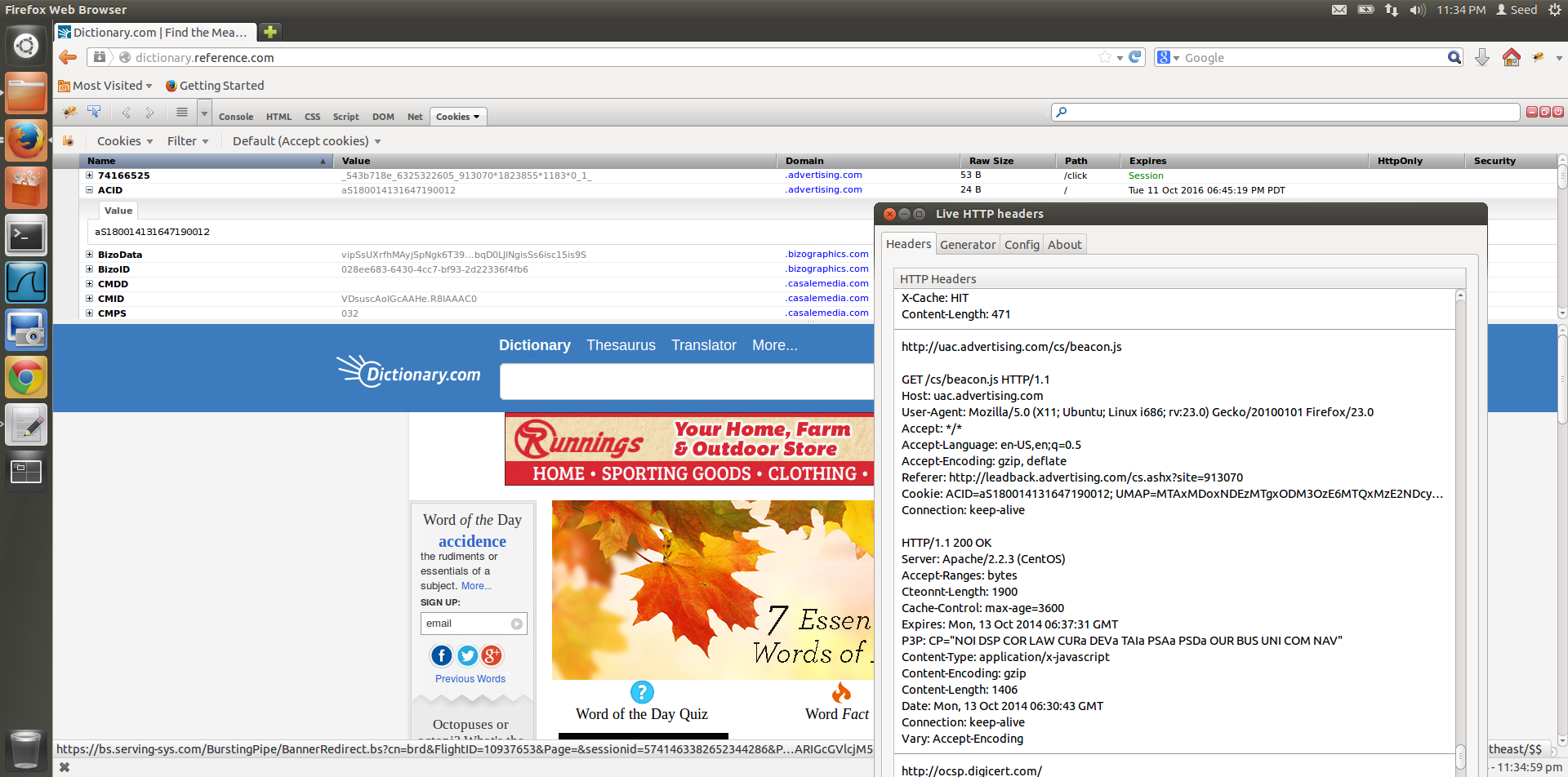
Regular window, ad displayed

**Figure 5.4**

**Observations and Explanation:**

1. When we open the browser in Private browsing mode and open [www.wtlabelgg.com](http://www.wtlabelgg.com) we get the home page and no ads, by seeing the LiveHTTPHeader, we can see that even though the ad server comes into action, here is no cookie created or returned. No ad is displayed also.
2. When we open the e-commerce website such as [www.wtshoestore.com](http://www.wtshoestore.com) and view the product details of a shoe, then the ad server website sets the cookie and then utilizes this cookie to display ads on the elgg website. In Private browsing also, cookies are set, but only till the private browser window is open, as soon as this window is closed the cookies that have been set are removed, thus maintaining the privacy of the user.
3. When we re-open private browsing after closing all the private browsing windows, we see that the ads are not displayed even though by looking at the live HTTP headers we can see that a request is sent to the ad server website, but since no cookies exist, no ad is displayed.
4. In task 1, we do not see any ads when we open the browser the 1st time after clearing the history, because no cookies have been set by any websites, after browsing e-commerce website, the third-party cookie is set and when we open elgg, we are able to see the ad of the item we were just viewing. When we close all the windows and re-open [www.wtlabelgg.com](http://www.wtlabelgg.com) we still see the ad being displayed, this is different from the private browsing window because in private browsing window all the stored information from the webpages such as cookies and temporary internet files are deleted for that session whereas in regular browsing, the stored information is left as it is, to be used by websites when the user accesses the internet again.
5. Figure 5.4 shows the comparison between a regular window and a private browsing window. Ad is displayed in regular window, whereas no ad is displayed in the private browsing window as a result of no cookie existing for the private browsing window.

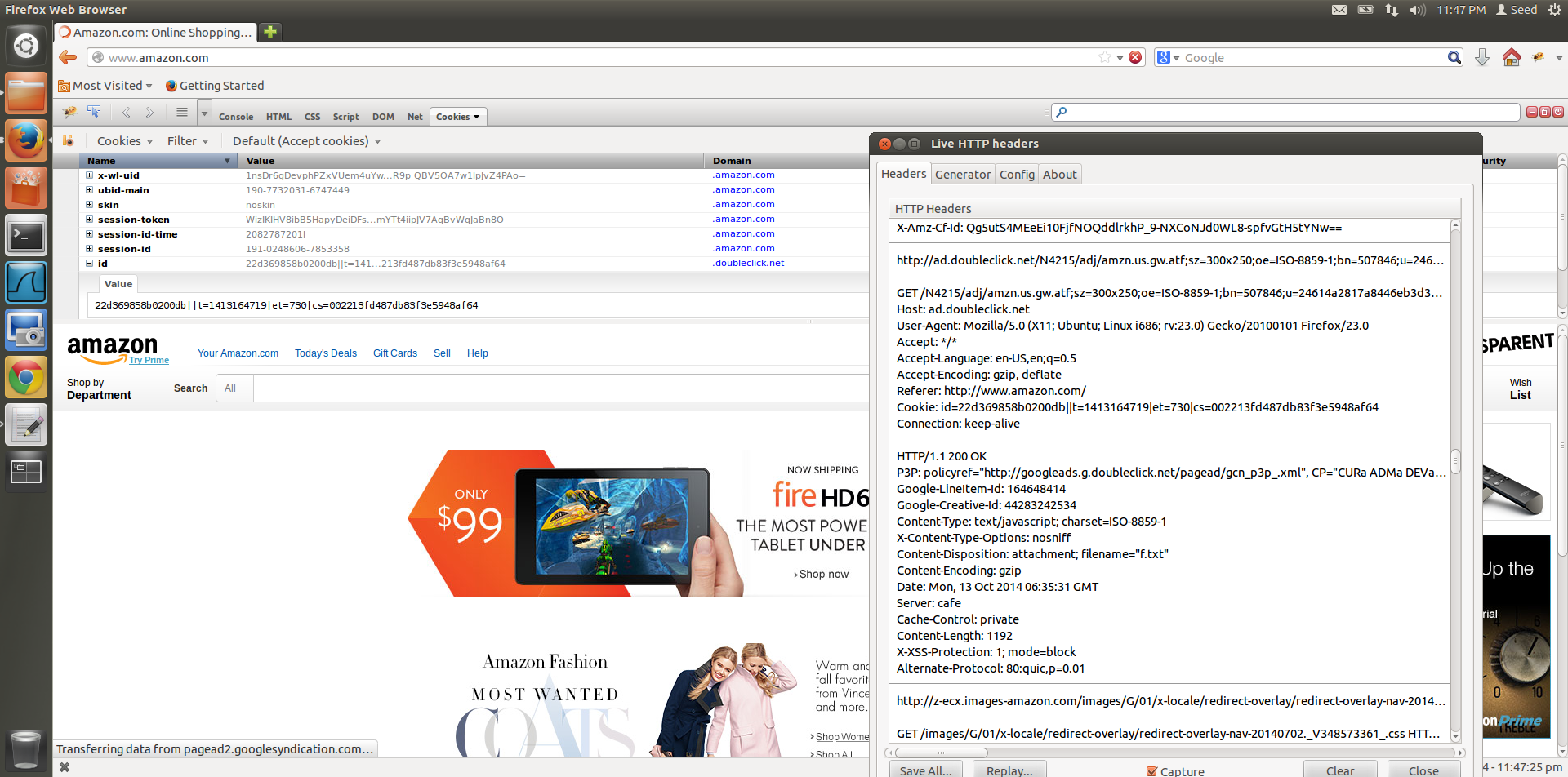
**Task 6:**

****

Third party cookie used for request

HTTP request to real world ad server

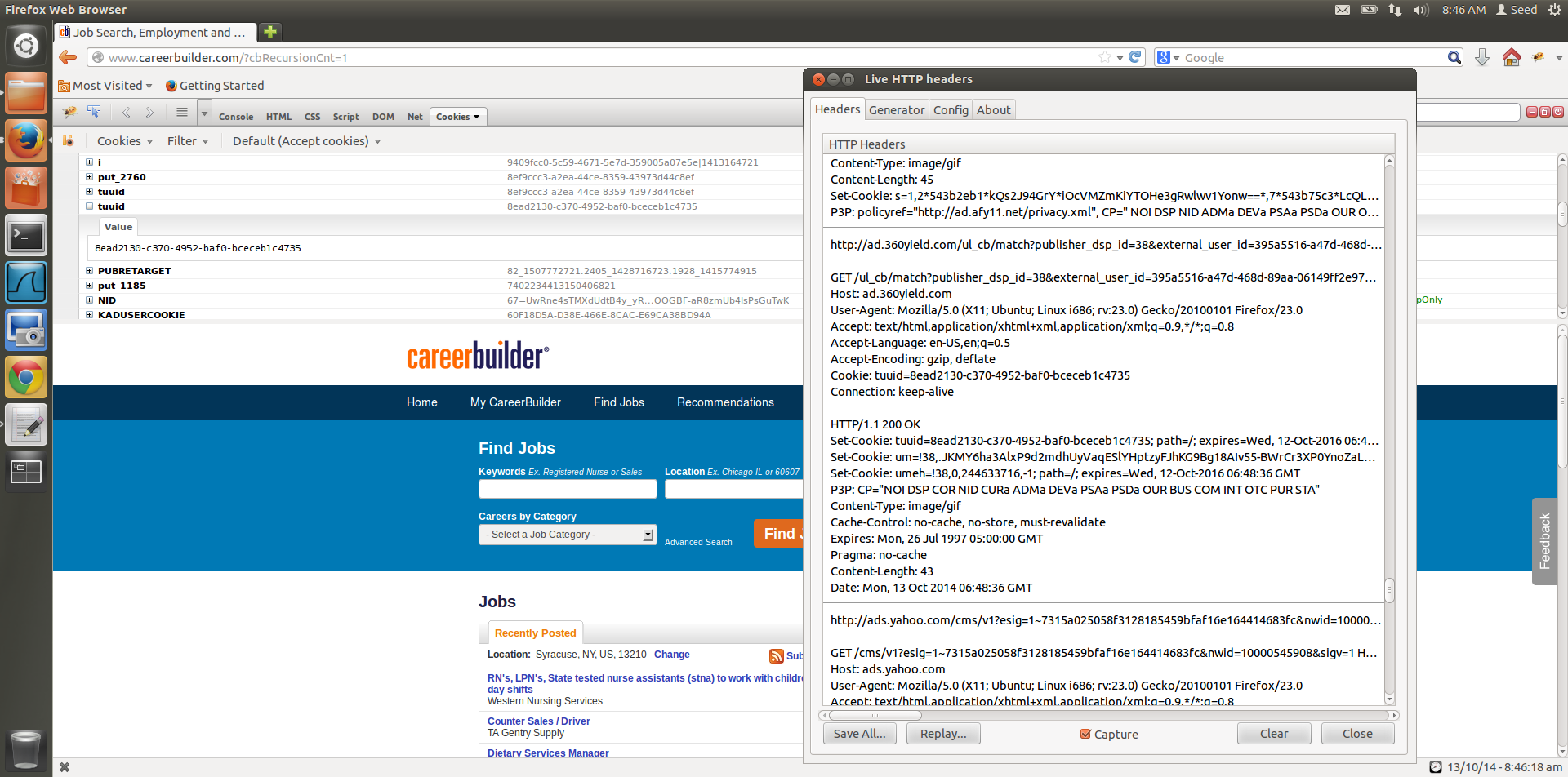
**Figure 6.1**

****

Third party cookie used for request

HTTP request to real world ad server

**Figure 6.2**

****

Third party cookie used for request

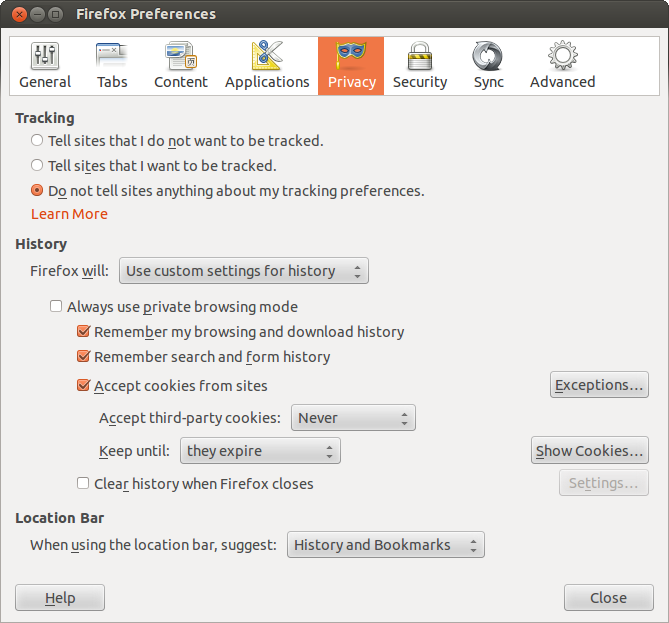
HTTP request to real world ad server

**Fi­­gure 6.3**

**Observations and Explanation:**

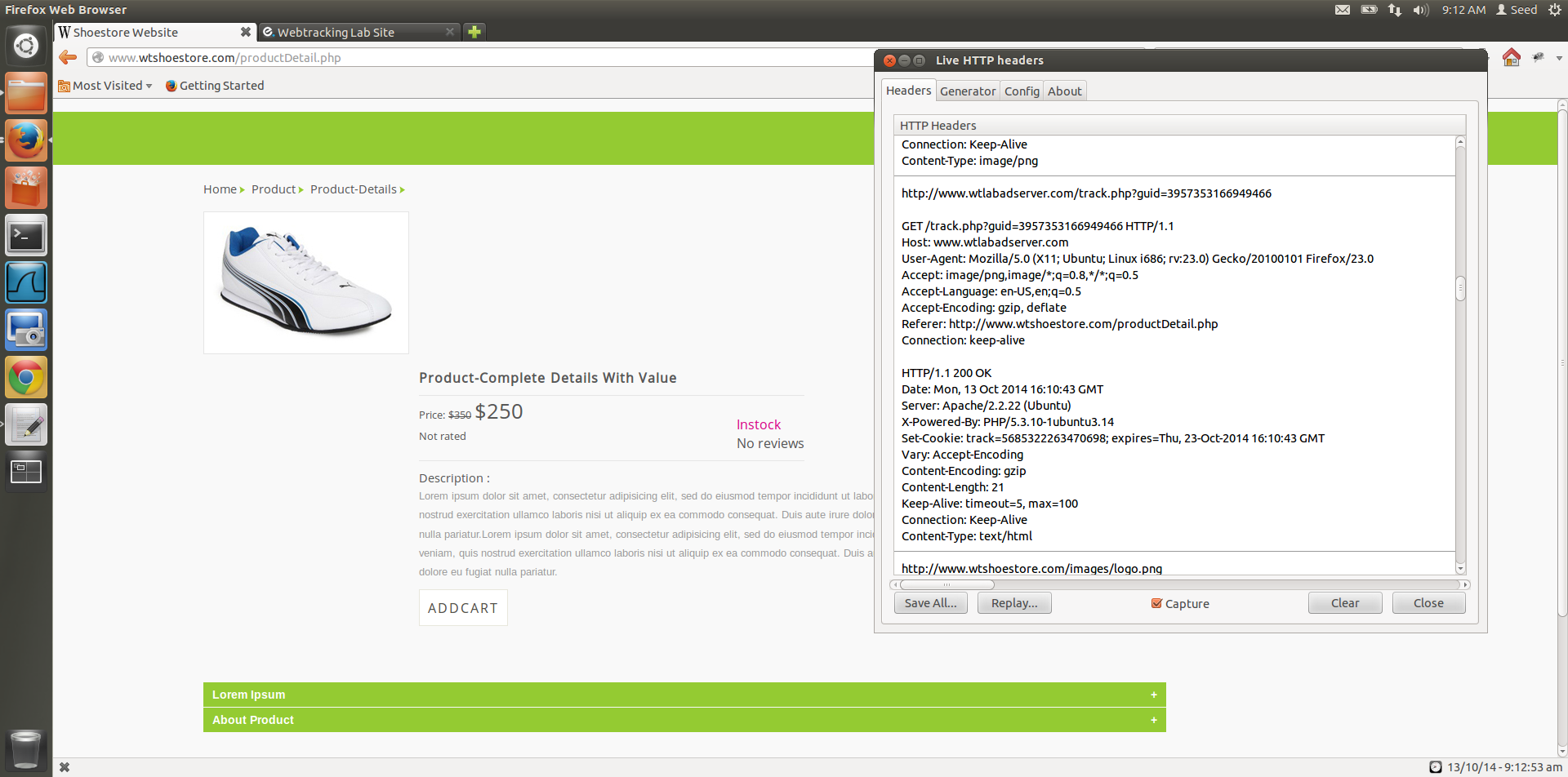
1. dictionary.reference.com- The third party cookie detected with name as ACID from the ad server uac.advertising.com as shown in Figure 6.1. Tools used are LiveHTTPHeader and FireBug to show the request header and the cookie.
2. amazon.com- The third party cookie detected with name as id from the ad server ad.doubleclick.net as shown in Figure 6.2. Tools used are LiveHTTPHeader and FireBug to show the request header and the cookie
3. careebuilder.com- The third party cookie detected with name as ACID from the ad server uac.advertising.com as shown in Figure 6.3. Tools used are LiveHTTPHeader and FireBug to show the request header and the cookie

**Task 7:**

****

Accepting third party cookies has been turned off

**Figure 7.1**

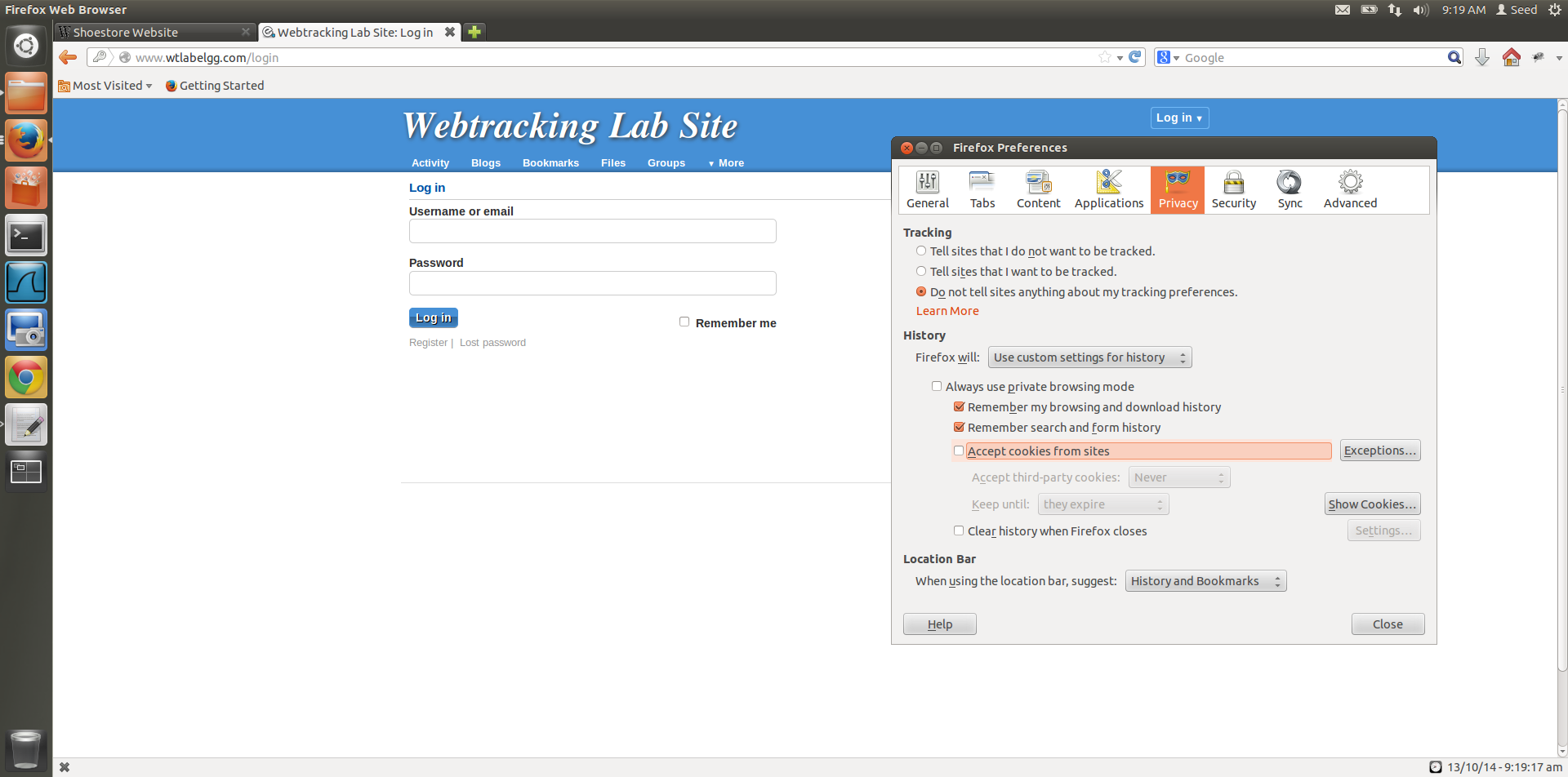
****

HTTP request that sets the third-party cookie

Missing cookie, as third-party cookies have been disabled

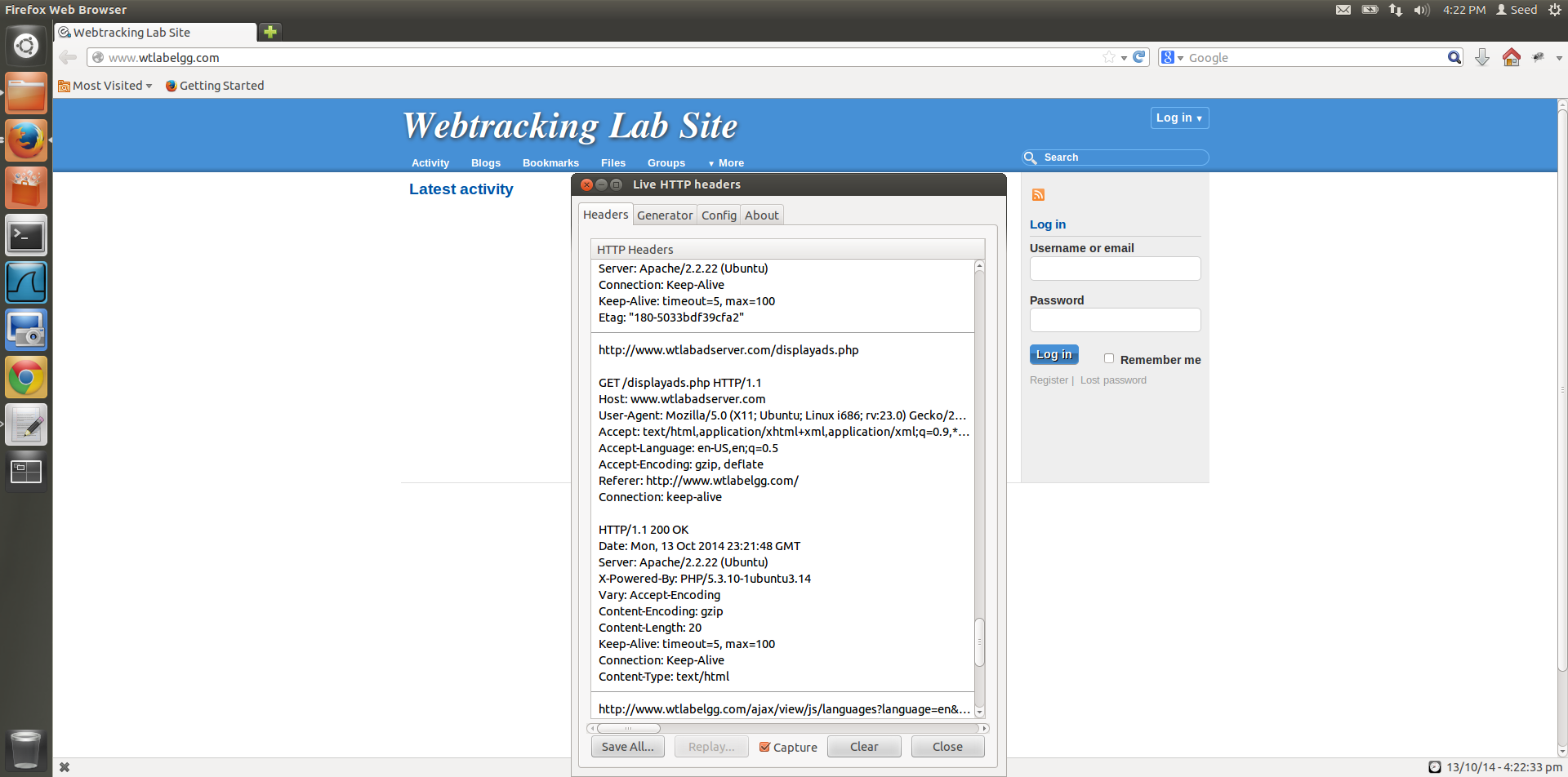
Request Header for third part website (wtlabadserver.com) after cookies have been turned off

**Figure 7.2**

****

Disabling cookies completely results in wtlabelgg, not being able to log in to the respective users website

**Figure 7.3**

****

Missing cookie name=value pair, as third-party cookies have been disabled

No ad displayed, third party cookies are disabled

Request Header from third part website to display ad (wtlabadserver.com) but cookies have been disabled

**Figure 7.4**

**Observations and Explanation:**

1. The request http header that is responsible for setting the cookies has been shown in Figure 7.2
2. The HTTP request to ad server from liveHTTPHeader is shown in Figure 7.4. No cookie name=value pair is seen in the header as third-party cookies have been disabled and so the webpages cannot ad third party cookies when they are accessed. This protection against web tracking is enforced by the browser.
3. In task 4 the HTTP request to ad server is based on the cookies being stored by 3rd party website [www.wtlabadserver.com](http://www.wtlabadserver.com) and so the ads are displayed based on the impressions count of the various products viewed by the user (Figure 4.2). In this task, since the third party cookies have been disabled, the ad server is not allowed to set the cookies when the user views product details, and since no cookies are set, there is no history of the user visiting the webpages. So, when the ad server wants to display ads, and it does not find any set cookies, no ads are displayed (Figure 7.4). LiveHTTPHeader capture shows that the cookies have not been set as the browser does not allow third-party cookies to be set.
4. From figure 7.3 it is also evident that wtlabelgg.com depends on cookies to function properly, as when we disable all forms of cookies, even first-party cookie, the website does not allow us to login to user alice with password seedalice, this is resolved when we enable cookies again.