

# Router Interrogation

---

Written by

Colby Lahaie

Researched by

David Paradise



The Senator Patrick Leahy Center for Digital Investigation

Champlain College

Date (Feb. 02, 2013)



**Disclaimer:**

*This document contains information based on research that has been gathered by employee(s) of The Senator Patrick Leahy Center for Digital Investigation (LCDI). The data contained in this project is submitted voluntarily and is unaudited. Every effort has been made by LCDI to assure the accuracy and reliability of the data contained in this report. However, LCDI nor any of our employees make no representation, warranty or guarantee in connection with this report and hereby expressly disclaims any liability or responsibility for loss or damage resulting from use of this data. Information in this report can be downloaded and redistributed by any person or persons. Any redistribution must maintain the LCDI logo and any references from this report must be properly annotated.*

**Contents**

- Contents ..... 1
- 1 Introduction..... 2
  - 1.1 Background..... 2
  - 1.2 Terminology..... 2
  - 1.3 Research Questions..... 2
- 2 Methodology and Methods ..... 3
  - 2.1 Data Collection ..... 3
  - 2.2 Analysis..... 4
- 3 Results..... 6
- 4 Conclusion ..... 8
- 5 Further Work..... 9
- 6 References..... **Error! Bookmark not defined.**



## 1 Introduction

This research project will explore the forensic data that can be retrieved from home routers. Routers are an important part of every investigation as they connect all of the local devices together in a local network. Routers are everywhere, in almost every home; they are the main component that connects and allows a computer to access the outside world. In this project we will be trying to determine exactly what type of information is stored on routers and if this information can be retrieved and used in an investigation. We also used Cain & Abel to go beyond the information stored directly on the router to see if it is possible to obtain other pertinent data that could be used during a live investigation.

### 1.1 Background

Router interrogation is analyzing a router for pertinent information that could potentially be used as evidence in a case. Investigators will look for different types of routers in the area, which could be hidden or visible, and see what devices are connected to that router. They can find out information about the computer such as, the name, or the nickname, of the connected device, the IP address assigned to the device, and the MAC address of the device. Additionally, investigators can use different software to capture packets, which can contain information on the system the user used, the user's internet history, email messages, social activity, etc.

There really hasn't been any research that we could find on interrogation of routers for digital forensic purposes.

### 1.2 Terminology

We are going to be conducting research on router interrogation; trying to find what data/evidence is directly stored on the router and what evidence can be gathered from the router, as a gateway, using other software.

**Address Resolution Protocol (ARP)** – Protocol for mapping an IP address to the hardware addresses in the local network.

**Dynamic Host Configuration Protocol (DHCP)** – Network protocol that allows a server to automatically assign an IP address to a computer from a collection of available IP addresses taken from the Internet Service Provider (ISP) or router. When a system is started, an IP address is assigned by the DHCP.

**Gateway** – A network point that acts as an entrance or access point to another network via software and hardware.

**Internet Protocol (IP) Address** – A unique string of numbers assigned to a device attached to a computer network and the Internet. It is an identifier of networked devices.

**Media Access Control (MAC) Address** – A unique identifier assigned to network devices for communication on the physical network. Every digital device has a unique MAC address. It is also known as a hardware or physical address.

**Packet** – Piece of data sent between a device and a destination on the network and Internet.

**Router** – A small physical device that joins multiple networks together; forwards data from one network to another. It allows communication between a local network and the Internet.

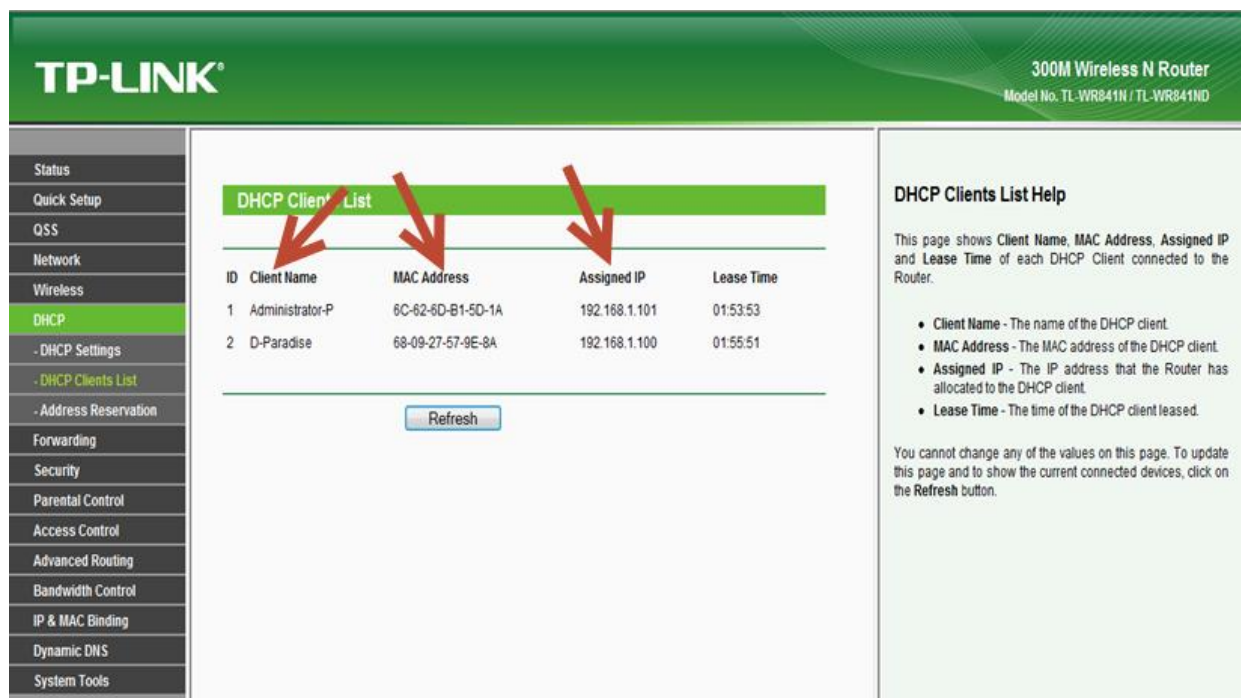
### 1.3 Research Questions

1. What data is or is not directly stored on a router?
2. What software can be used to obtain information from routers?
3. What information can be obtained from data directly stored on a router using other software?
4. What data can be captured by other software using the router as a gateway?

## 2 Methodology and Methods

We first started out by using the router that Burlington Telecom sent to us and accessing its webpage GUI (Graphical User Interface) to see what information was stored on the router itself. The only information that we were able to obtain was the names of the connected devices, the MAC address, and the IP address of the connected devices, as well as the total time that the device had been connected to the router (2.1.1). Inside of the router website GUI, under the DHCP tab (Dynamic Host Configuration Protocol), you can find the client name for any device accessing the router and what the IP and MAC address of the connected device was.

### 2.1.1 TP-LINK Website GUI



ID	Client Name	MAC Address	Assigned IP	Lease Time
1	Administrator-P	6C-62-6D-B1-5D-1A	192.168.1.101	01:53:53
2	D-Paradise	68-09-27-57-9E-8A	192.168.1.100	01:55:51

**DHCP Clients List Help**

This page shows Client Name, MAC Address, Assigned IP and Lease Time of each DHCP Client connected to the Router.

- **Client Name** - The name of the DHCP client.
- **MAC Address** - The MAC address of the DHCP client.
- **Assigned IP** - The IP address that the Router has allocated to the DHCP client.
- **Lease Time** - The time of the DHCP client leased.

You cannot change any of the values on this page. To update this page and to show the current connected devices, click on the Refresh button.

With the lack of information we moved on to use Cain & Abel, a freeware password recovery tool for windows. Cain & Abel isn't used to pull information from the router's memory like the router's webpage GUI, but instead to take the information directly from the target computer connected to the router. The reason we used Cain & Abel was because there is not a lot of software that can obtain information from routers. The software that is available is not readily available to the public. Router Marshall, for instance, is only available to U.S. Law Enforcement personnel free of charge.

Having Cain & Abel installed on LCDI Testing Computer 3 and a wired connection to Workstation 11 through the router, we were able to generate data on Workstation 11 that would show up in the logs on LCDI Testing Computer 3. We also used the Wireless Scanner tool within Cain & Abel to obtain information from the router such as, user ID's, passwords, and specific dates and times of when it was used/accessed.

## 2.2 Data Collection

Item	Identifier	Size / Specifications
Test Computer 1	LCDI Testing Computer 3	Running Cain & Abel – compatible w/ Windows NT, 2000, XP, Vista or Windows 7  Specs – Pentium Dual-Core CPU E6500 @ 2.93GHz w/4GB Memory, Windows 7



<i>Test Computer 2</i>	<i>Workstation 11</i>	<i>Specs – Intel Core 2 Quad CPU Q9450 @ 2.66GHz w/6GB Memory, Windows 7 SP1</i>  <i>Google Chrome Version 24.0.1312.57</i>  <i>Firefox Version 19.0</i>  <i>Opera Version 12.14</i>  <i>Internet Explorer Version 9.0.8112.16421</i>
<i>Burlington Telecom.</i>  <i>Test TP-LINK Router</i>	<i>LCDI-EA-001</i>	<i>TP-LINK TL-WR841N v6/v7</i>  <i>IEEE 802.11n, IEEE 802.11g, IEEE 802.11b</i>  <i>Compatible with Windows 98SE, NT, 2000, XP, Vista or Windows 7, MAC OS, NetWare, UNIX or Linux.</i>  <i>Running on Windows 7 computer</i>  <i>Firmware – 3.12.5 Build 100929 Rel.57776n</i>  <i>Frequency - 2.4-2.4835GHz</i>

### 2.3 Analysis

We first linked the test TP-LINK Router (LCDI-EA-001) to the internet with an Ethernet cable and then proceeded to use 2 more Ethernet cables to link up LCDI Testing Computer 3, running Cain & Abel, and Workstation 11 that we ran the web browser on to gather information. When that was all hooked up, we started up Cain & Abel on LCDI Testing Computer 3 and turned on the sniffer. In the tab labeled Sniffer, we right clicked and selected “Scan MAC Addresses”. After selecting the Network Interface Card, we scanned the network for the other computer that we would be running the test on. Then, we selected the router IP address then the Computer’s IP address, that way all of the traffic would be routed through the test computer before it goes out to the internet. Once that was set up, we selected the ARP poisoning button to start gathering the data. When the data started to be collected, we went to the Passwords tab where we could see specific websites accessed, such as tumblr.com or reddit.com, and if it were an unsecured router or website, we could see e-mail and passwords used to log in (See 2.3.1 below).

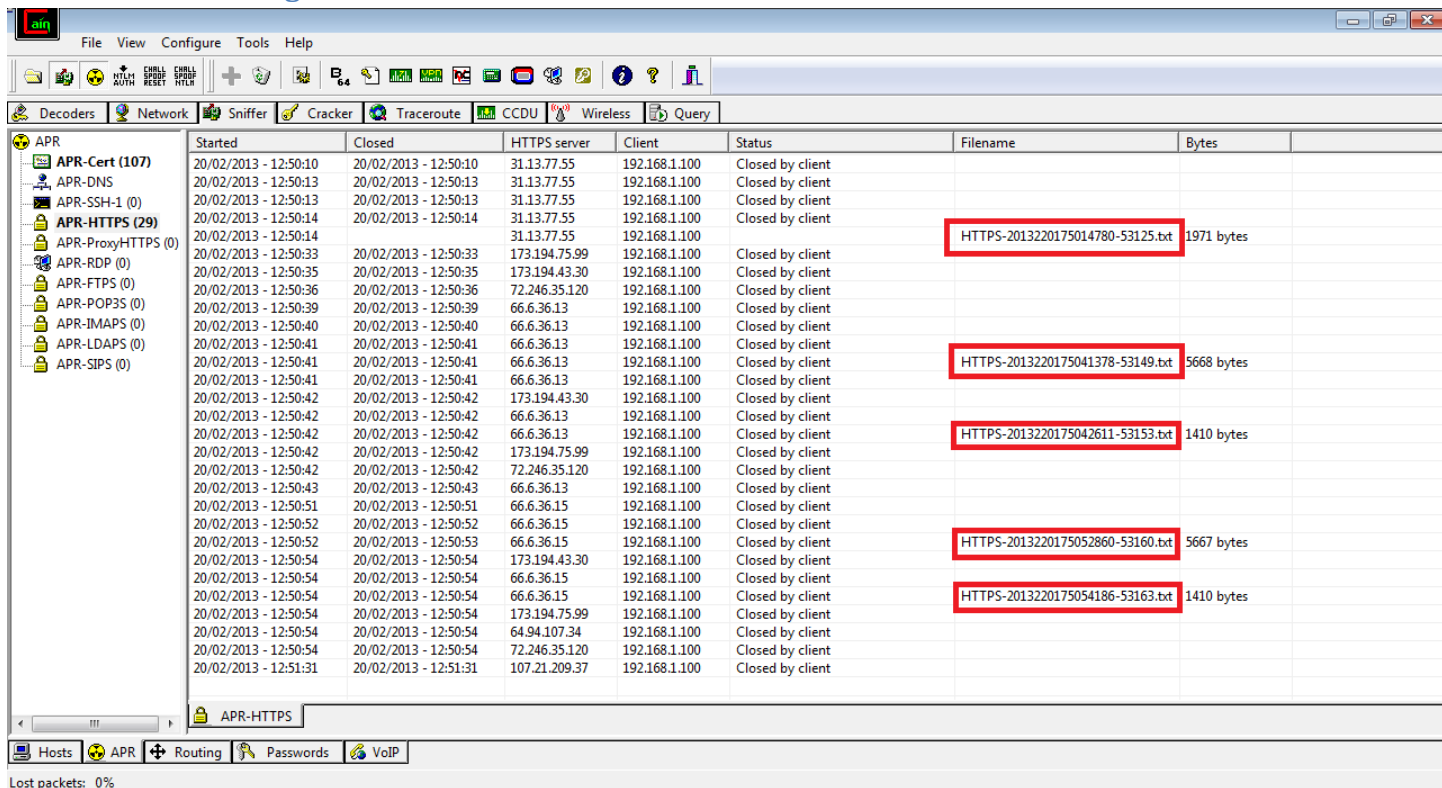
### 2.3.1 Websites Accessed

Timestamp	HTTP server	Client	Username	Password	URL
28/01/2013 - 14:36:30	74.125.226.231	192.168.1.101	377573293	1903x923	http://www.reddit.com/
28/01/2013 - 14:37:51	65.55.253.27	192.168.1.100	fb:fb, tw:fw	hops	http://www.msn.com/?ocid=iehp
28/01/2013 - 14:37:51	64.4.21.39	192.168.1.100	86c4368ba53f4...	http://www.m...	http://www.msn.com/?ocid=iehp
28/01/2013 - 14:37:52	65.55.121.231	192.168.1.100	02B80FF5562D...	1089 HTTP/1.1	http://www.msn.com/?ocid=iehp
28/01/2013 - 14:37:52	65.55.253.27	192.168.1.100	86c4368ba53f4...	False	http://www.msn.com/?ocid=iehp
28/01/2013 - 14:37:52	216.38.160.139	192.168.1.100	1	0.0.0.0	http://www.msn.com/?ocid=iehp
28/01/2013 - 14:37:52	65.55.121.231	192.168.1.100	02B80FF5562D...	1455 HTTP/1.1	http://www.msn.com/?ocid=iehp
28/01/2013 - 14:37:52	65.55.121.231	192.168.1.100	02B80FF5562D...	1455 HTTP/1.1	http://www.msn.com/?ocid=iehp
28/01/2013 - 14:37:52	65.55.121.231	192.168.1.100	02B80FF5562D...	1089 HTTP/1.1	http://www.msn.com/?ocid=iehp
28/01/2013 - 14:37:53	65.55.121.231	192.168.1.100	02B80FF5562D...	1455 HTTP/1.1	http://www.msn.com/?ocid=iehp
28/01/2013 - 14:37:55	216.38.160.139	192.168.1.100	iehp	0	http://www.msn.com/?ocid=iehp
28/01/2013 - 14:37:56	65.55.253.27	192.168.1.100	default	hops	http://www.msn.com/?ocid=iehp
28/01/2013 - 14:37:56	74.125.226.232	192.168.1.100	448692061	1263x929	http://twitter.com/
28/01/2013 - 14:38:05	74.125.226.232	192.168.1.100	1807017759	1280x929	http://www.tumblr.com/
28/01/2013 - 14:38:07	74.125.226.232	192.168.1.100	397314527	1280x929	http://www.reddit.com/
28/01/2013 - 14:38:20	74.125.226.232	192.168.1.100	405096457	1280x929	http://www.reddit.com/
28/01/2013 - 14:38:23	74.125.226.232	192.168.1.100	2073512952	1263x929	http://www.reddit.com/
28/01/2013 - 14:38:25	74.125.226.232	192.168.1.100	1314469871	1280x929	http://www.reddit.com/
28/01/2013 - 14:38:26	74.125.226.232	192.168.1.100	1710351205	1280x929	http://www.reddit.com/
28/01/2013 - 14:38:29	74.125.226.232	192.168.1.100	216473016	1280x929	http://www.reddit.com/

The ARP tab shows the data you get from the ARP Poisoning attack (see Figure 2.3.2). This is where one can locate the logs that show in depth detail about websites accessed. Under Filename at the top will show some of the captures will have a text file labeled with HTTPS followed by a string of numbers. Right clicking on these logs will access where the files are located and will all the events of the generated logs.

This poisoning takes advantage of an exploit in the ARP that has the host computer act as a gateway between the target computer and the router, gaining access to the flow of packets being sent and received over the network, and this tab records this network traffic in a log. Most of the browsers work differently when it comes to encryption and how they send data, for example, I was able to get a username and password for a fake tumblr.com account on the Firefox browser but on Google chrome I was unable to get the password for the same account. Using a newly generated e-mail on shortmail.com, I was able to capture an e-mail being sent to another one of my accounts. In the log for that e-mail it gives me a detailed description of who I was sending it to, the time it was sent, the subject heading, and the content of the e-mail itself.

### 2.3.2 ARP Poisoning Attack

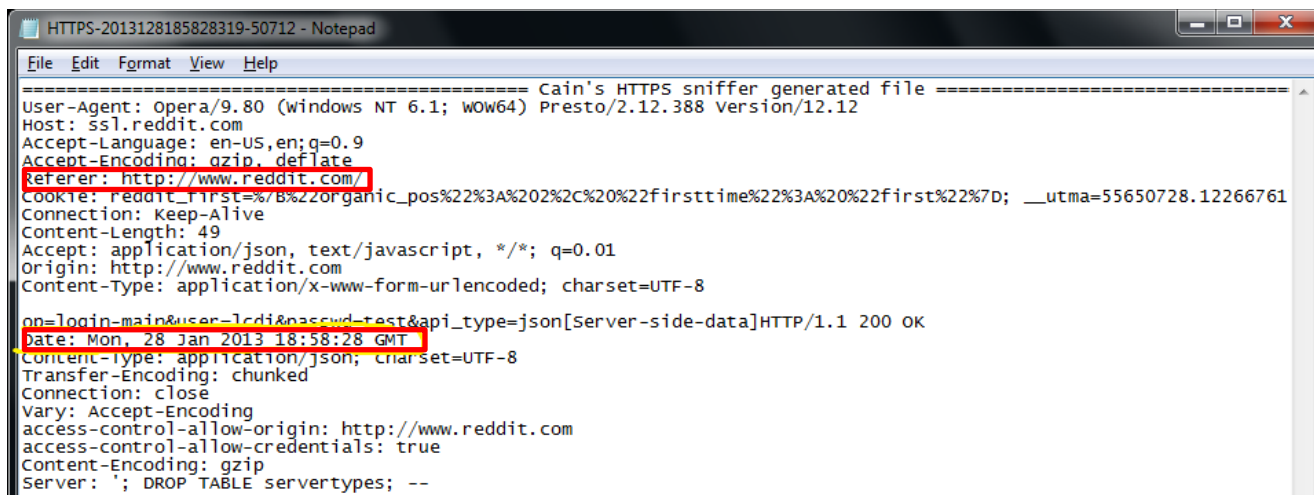


Started	Closed	HTTPS server	Client	Status	Filename	Bytes
20/02/2013 - 12:50:10	20/02/2013 - 12:50:10	31.13.77.55	192.168.1.100	Closed by client		
20/02/2013 - 12:50:13	20/02/2013 - 12:50:13	31.13.77.55	192.168.1.100	Closed by client		
20/02/2013 - 12:50:13	20/02/2013 - 12:50:13	31.13.77.55	192.168.1.100	Closed by client		
20/02/2013 - 12:50:14	20/02/2013 - 12:50:14	31.13.77.55	192.168.1.100	Closed by client		
20/02/2013 - 12:50:14	20/02/2013 - 12:50:14	31.13.77.55	192.168.1.100	Closed by client	HTTPS-2013220175014780-53125.txt	1971 bytes
20/02/2013 - 12:50:33	20/02/2013 - 12:50:33	173.194.75.99	192.168.1.100	Closed by client		
20/02/2013 - 12:50:35	20/02/2013 - 12:50:35	173.194.43.30	192.168.1.100	Closed by client		
20/02/2013 - 12:50:36	20/02/2013 - 12:50:36	72.246.35.120	192.168.1.100	Closed by client		
20/02/2013 - 12:50:39	20/02/2013 - 12:50:39	66.6.36.13	192.168.1.100	Closed by client		
20/02/2013 - 12:50:40	20/02/2013 - 12:50:40	66.6.36.13	192.168.1.100	Closed by client		
20/02/2013 - 12:50:41	20/02/2013 - 12:50:41	66.6.36.13	192.168.1.100	Closed by client		
20/02/2013 - 12:50:41	20/02/2013 - 12:50:41	66.6.36.13	192.168.1.100	Closed by client	HTTPS-2013220175041378-53149.txt	5668 bytes
20/02/2013 - 12:50:41	20/02/2013 - 12:50:41	66.6.36.13	192.168.1.100	Closed by client		
20/02/2013 - 12:50:42	20/02/2013 - 12:50:42	173.194.43.30	192.168.1.100	Closed by client		
20/02/2013 - 12:50:42	20/02/2013 - 12:50:42	66.6.36.13	192.168.1.100	Closed by client		
20/02/2013 - 12:50:42	20/02/2013 - 12:50:42	66.6.36.13	192.168.1.100	Closed by client	HTTPS-2013220175042611-53153.txt	1410 bytes
20/02/2013 - 12:50:42	20/02/2013 - 12:50:42	173.194.75.99	192.168.1.100	Closed by client		
20/02/2013 - 12:50:42	20/02/2013 - 12:50:42	72.246.35.120	192.168.1.100	Closed by client		
20/02/2013 - 12:50:43	20/02/2013 - 12:50:43	66.6.36.13	192.168.1.100	Closed by client		
20/02/2013 - 12:50:51	20/02/2013 - 12:50:51	66.6.36.15	192.168.1.100	Closed by client		
20/02/2013 - 12:50:52	20/02/2013 - 12:50:52	66.6.36.15	192.168.1.100	Closed by client		
20/02/2013 - 12:50:52	20/02/2013 - 12:50:53	66.6.36.15	192.168.1.100	Closed by client	HTTPS-2013220175052860-53160.txt	5667 bytes
20/02/2013 - 12:50:54	20/02/2013 - 12:50:54	173.194.43.30	192.168.1.100	Closed by client		
20/02/2013 - 12:50:54	20/02/2013 - 12:50:54	66.6.36.15	192.168.1.100	Closed by client		
20/02/2013 - 12:50:54	20/02/2013 - 12:50:54	66.6.36.15	192.168.1.100	Closed by client	HTTPS-2013220175054186-53163.txt	1410 bytes
20/02/2013 - 12:50:54	20/02/2013 - 12:50:54	173.194.75.99	192.168.1.100	Closed by client		
20/02/2013 - 12:50:54	20/02/2013 - 12:50:54	64.94.107.34	192.168.1.100	Closed by client		
20/02/2013 - 12:50:54	20/02/2013 - 12:50:54	72.246.35.120	192.168.1.100	Closed by client		
20/02/2013 - 12:51:31	20/02/2013 - 12:51:31	107.21.209.37	192.168.1.100	Closed by client		

### 3 Results

Cain and Abel generates text files of the packet content that has been “sniffed” by the program. The data that is captured depends on the internet browser used and the whether or not the browser or other online application uses encryption to obscure and protect the data. The file shows the date and time that an action occurred and what website was accessed. The below screen capture (3.1.1) shows that someone accessed the website www.reddit.com on January 28<sup>th</sup> (Monday), 2013 at 18:58 GMT (6:58 PM).

#### 3.1.1 Date and Time



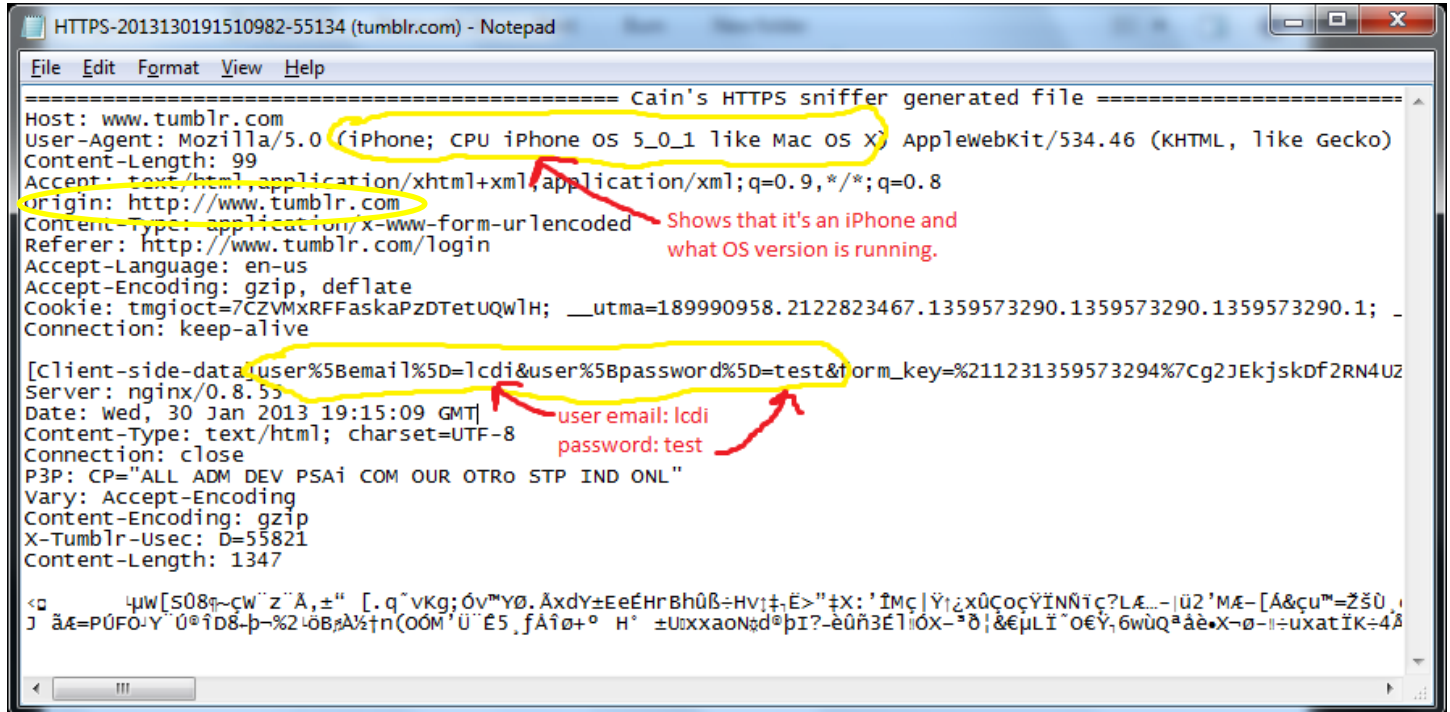
```

----- Cain's HTTPS sniffer generated file -----
User-Agent: opera/9.80 (windows NT 6.1; wow64) Presto/2.12.388 version/12.12
Host: ssl.reddit.com
Accept-Language: en-US,en;q=0.9
Accept-Encoding: gzip, deflate
Referer: http://www.reddit.com/
Cookie: reddit_first=/B%2Zorganic_pos%22%3A%20%2C%20%22firsttime%22%3A%20%22first%22%7D; __utma=55650728.12266761
Connection: Keep-Alive
Content-Length: 49
Accept: application/json, text/javascript, */*; q=0.01
Origin: http://www.reddit.com
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

op=login-main&user=lcidi&passwd=test&api_type=json[Server-side-data]HTTP/1.1 200 OK
Date: Mon, 28 Jan 2013 18:58:28 GMT
Content-type: application/json; charset=UTF-8
Transfer-Encoding: chunked
Connection: close
Vary: Accept-Encoding
access-control-allow-origin: http://www.reddit.com
access-control-allow-credentials: true
Content-Encoding: gzip
Server: '; DROP TABLE servertypes; --
    
```

The generated text files by Cain and Abel also has the ability to report what operating system the computer or mobile device was using at the time the action occurred. It also has the ability to capture the username and password of certain websites. The below screen capture (3.1.2) shows that the device used was an iPhone and used iOS 5.0.1. It also shows that we accessed www.tumblr.com, using a fake e-mail and password, which was capture by Cain and Abel. The fake e-mail used was "lcdi" and the password was "test".

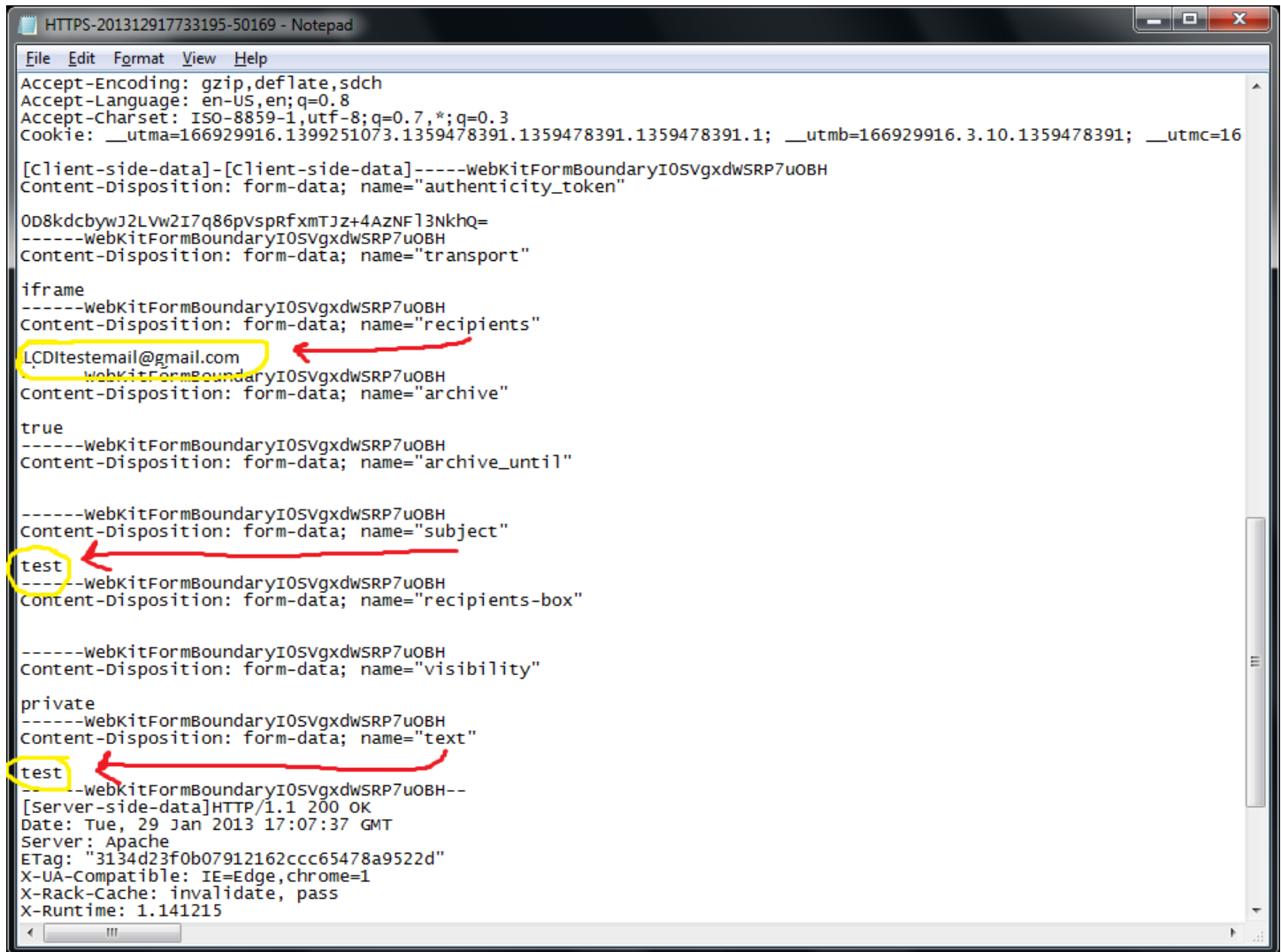
### 3.1.2 Operating systems and log-in data



Cain and Abel also has the ability to capture certain email information, such as the email subject header and the target email address. The below screen capture (3.1.3) is of a test e-mail capture. The results showed that we were able to attain the target e-mail address, the subject and the text, which was the actual contents of the email that we sent, meaning that an investigator could capture the entire message of the email body. The data obtained, again depends on whether or not the web application visited is using encryption or not. Based on the data we were able to retrieve, it does not look like this Gmail was using encryption.



### 3.1.3 Acquiring E-mail information



```
HTTPS-201312917733195-50169 - Notepad
File Edit Format View Help
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
Cookie: __utma=166929916.1399251073.1359478391.1359478391.1359478391.1; __utmb=166929916.3.10.1359478391; __utmc=16

[Client-side-data]-[Client-side-data]-----WebKitFormBoundaryI05vgxdwSRP7uOBH
Content-Disposition: form-data; name="authenticity_token"

0D8kdcbywJ2Lvw2I7q86pVsprfxmTJz+4AZNF13NkhQ=
-----WebKitFormBoundaryI05vgxdwSRP7uOBH
Content-Disposition: form-data; name="transport"

iframe
-----WebKitFormBoundaryI05vgxdwSRP7uOBH
Content-Disposition: form-data; name="recipients"
LCDItestemail@gmail.com
-----WebKitFormBoundaryI05vgxdwSRP7uOBH
Content-Disposition: form-data; name="archive"

true
-----WebKitFormBoundaryI05vgxdwSRP7uOBH
Content-Disposition: form-data; name="archive_until"

-----WebKitFormBoundaryI05vgxdwSRP7uOBH
Content-Disposition: form-data; name="subject"
test
-----WebKitFormBoundaryI05vgxdwSRP7uOBH
Content-Disposition: form-data; name="recipients-box"

-----WebKitFormBoundaryI05vgxdwSRP7uOBH
Content-Disposition: form-data; name="visibility"

private
-----WebKitFormBoundaryI05vgxdwSRP7uOBH
Content-Disposition: form-data; name="text"
test
-----WebKitFormBoundaryI05vgxdwSRP7uOBH--
[Server-side-data]HTTP/1.1 200 OK
Date: Tue, 29 Jan 2013 17:07:37 GMT
Server: Apache
Etag: "3134d23f0b07912162ccc65478a9522d"
X-UA-Compatible: IE=Edge,chrome=1
X-Rack-Cache: invalidate, pass
X-Runtime: 1.141215
```

## 4 Conclusion

After conducting this research we found that there is not much data stored on a router; however, different routers could potentially store different data. From the router that we were provided, we only were able to retrieve data directly linked to the connected computers. This data consisted of the assigned IP address of the connected computer, the computer name (or nickname), the MAC address of the computer, and the total time that the devices had been connected to the router.

Since we were unable to get much from the router via its webpage interface, we had to resort to using another outside tool (Cain and Abel) to try and retrieve other data that might be stored on a router. We found that we were able to obtain the same type of information directly stored on the router, as we did with the router's webpage interface. This data also consisted of the device connected to the network, the MAC address, the IP address, and how much data was being used by the device. Since we were only able to find such limited data, we used Cain and Abel to do a further in depth analysis to use the router as a gateway to capture and analyze the packets sent and received by the connected devices. After conducting this analysis, we were able to find emails, email addresses, some passwords, web history, and the date and time the person accessed the sites.



## **5 Further Work**

We were unable to get the Law Enforcement tool Router Marshal, so if we were able to get it in the future, we could use it to verify our results and conduct this research with an actual digital forensics tool for router interrogation. We could also try it with other software, such as Wireshark, that has the ability to capture packets and conduct more in depth analysis of the packets. We also need to research different types of routers because there are many.