Network Forensics Challenge Report

Héctor F. Jiménez Saldarriaga
@c1b3rh4ck

PCAP Network Packet Capture Analysis

This page is intentionally left blank

Contents

Network Forensics Challenge
BarcampSE v4.0 2013

c1b3rh4ck c1b3rh4ck@gmail.com
Hector Fabio Jiménez S.

December 8, 2013

Abstract

CTFs and Jeopardy contest have been increasing in the last five years,in every security event always are ways to mount a challenge,this report tries to sumarize the solutions for the BarcampSE v4.0 hosted by Barcampse.org,at this scenario we have a network forensics situation.I need to clarify that I'm a Enthusiast you need to asume that I am not an expert on this field 'Network Forensics' just a security enthusiast. However I can try to learn something new for this experience, so I hope you enjoy this try of report :).

1 Introduction

Network forensics involves the identification, preservation, and analysis of evidence of attacks in order to identify the attackers and document their activity with sufficient reliability to justify appropriate technological, business, and legal responses.
Packet capture is widely used in network security tools to analyze raw traffic for detecting malicious behaviour (scans and attacks), sniffing, fingerprinting and many other (often devious) uses.
To analyze this scenario I have followed the Forensic Process describe in NIST **SP 800-86** the publication itself describes the processes for performing effective forensics activities and recommends ways to use the many data sources that are available for **identification, collection, examination, analysis, reporting** Forensic techniques.
We've got up 6 Packet captures in order to analyze and answer 5 different question. Following the procedure we need to gather the in from the website in order to adquire the proper information.

Figure 1:Announcement.

Finishing the download of all files, understanding the terms to apply and qualification methodology,at this point I have a working directory copy of the network forensics challenge specifically the packet captures. Following the Forensic Process describe in NIST SP 800-86 with need to follow four-step process for applying digital forensic techniques in a consistent manner:

1. Collection.
2. Examination.
3. Analysis.
4. Reporting.

2 Executive Summary

The purpose of this report is to analyse and report the contents of 6 network captures file which is an archive containing the network based activities monitored on a given networks. This file was downloaded on a local hard drive before carrying out the analysis. The network is reported to contain the activities of an different devices on a host network. The analysis attempts to reconstruct the structure of the network, identify key players in the network and determine all activities leading to and occurring during activities monitored. The analysis was carried out mainly using network forensic tools such as Wireshark and others please refer to 7 . Some key findings from the analysis are listed below. Each of these findings has been elaborated with supporting evidence documents in Sections of the Details of each Network capture.

2.1 Chronology

Chronology is the science of arranging events in their order of occurrence in time.According to Lexis Nexis From the starting gate to the finish line, assembling case facts in an accessible format can put you on track to courtroom victory,this takes effect with the Digital forensic analysis. For this analysis we have 6 Network captures,each one with his own date of start and finish,lets take a look a the next table.

Date	Hour	Capture Number
2012-11-27	10:15:24	1
2012-11-27	10:27:20	1
2012-11-29	20:15:57	3a
2012-11-29	20:16:36	3a
2012-11-29	20:16:43	3b
2012-11-29	20:18:21	3b
2012-11-29	21:50:15	2a
2012-11-29	21:51:58	2a
2012-11-29	21:50:11	2b
2012-11-29	21:52:04	2b

In the previous table you can see 4 network capture in order of occurrence, the first capture was at 10:15:24 and finish was 10:27:20 this corresponds to CAPTURA1.cap.This date was extracted from the wireshark summary, and the same process to all packet captures file.
CAPTURA4.cap was not taken into account, because it did not involve actors from previous network captures and not related to mac addresses, the network capture has nothing to do with previous catches,dates are not consistent as a year after,also the events in CAPTURA4.cap were:

2013-07-25 01:18:20 4
2013-07-25 01:19:28 4

This file is discarded by chronology.

1. In the Network Capture 1 shows the visit several websites, such as forensic tools, forensic crime magazines, also can be seen visiting various blogs. There were 4 devices identified in this capture :

   - **Cisco-Li_0c:7b:9c**
   - **MS-NLB-PhyServer**
   - **Apple_92:6e:3d**
   - **Ipv4mcast**

   The mos relevant capture was the conversation between Cisco-Li_0c:7b:9c identified with 63.245.217.112 and MS-NLB-PhyServer with ip 192.168.0.157.

2. In the Network Capture 2A there was multiple users and passwords, also failed attempts to Connect to a network device are observed, it appears that the network device is a trendnet tew_638 identified with PIZARRO ssid and password seczone2012.
   There were 5 devices identified in this capture :

   - **Trendnet_cf:8c:04**

- **Apple_19:0c:b7**
- **Apple_92:6e:3d**
- **Apple_0e:bb:60**
- **Ipv4mcast_00:00:fb**
- **Ipv6mcast**

users were extracted using a base64 decoder.The mos relevant conversation was between: **Apple_19:0c:b7** identified with ip 192.168.10.99 and **Trendnet_cf:8c:04** with ip address 192.168.10.100.

3. CAPTURA2B.cap, In this capture I observed failed attempts from **Apple_19:0c:b7**, specifically 3 also shows that the Trendnet Device uses a web server known as Go ahead webserver with has a lot of vulnerabilities. Also can be seen that the team has some flaws in the sequences the (FCS) refers to the extra checksum added to a frame in a communications protocol for error detection.

4. In Capture 3A and 3B there were Remarkable amount of 802.11 deauth packets, an aireplay-ng attack. We don't know where the attack came from and also you cannot stop a bad guy from sending deauthentication packets it is due to the role model of wifi design.send deauth packets against the unique client connecte to AP, it was **Apple_92:6e:3d** bad guys captures a copy of the initial handshake this was demonstrate using aircrack-ng.

3 Collection

During collection, data related to a specific event is identified, labeled, recorded, and its integrity is preserved. to get started with,i've set up a virtual machine using virtualbox to use Debian Gnu/Linux tools, and as a guest machine I have used Windows 7 Enterprise SP1 the most important thing is be organized with the directories.After that I ran a file integrity tool over all pcaps,the integrity of the information and maintain a strict chain of custody for the data inside the packet capture.

```
root@HaDeS:/home/c1b3rh4ck/CTF/RetoForense# file CAPTURA{1..4}*.cap
CAPTURA1.cap:  pcap-ng capture file - version 1.0
CAPTURA2A.cap: tcpdump capture file (little-endian) - version 2.4 (Ethernet, capture length 65535)
CAPTURA2B.cap: pcap-ng capture file - version 1.0
CAPTURA3A.cap: tcpdump capture file (little-endian) - version 2.4 (802.11, capture length 65535)
CAPTURA3B.cap: tcpdump capture file (little-endian) - version 2.4 (802.11, capture length 65535)
CAPTURA4.cap:  tcpdump capture file (little-endian) - version 2.4 (Ethernet, capture length 65535)
root@HaDeS:/home/c1b3rh4ck/CTF/RetoForense# sha1sum CAPTURA{1..4}*.cap
0a49f96abbc6a4ec0a0f2d1886259fa6adb53999  CAPTURA1.cap
78a7e8ba4555bc4382a00e98baad8883a8a7ee44  CAPTURA2A.cap
95fa742a8272cf29359bb32ad26993ed8f473355  CAPTURA2B.cap
5a76ccec1cd78d66eab279b1627cda9d95b80840  CAPTURA3A.cap
93ad834089ef9e14abda4036c58eb7849323153a  CAPTURA3B.cap
795faee94ebc811654433949ca4aefd4f07a99aa  CAPTURA4.cap
root@HaDeS:/home/c1b3rh4ck/CTF/RetoForense#
```

Figure 1.1:Labeling and identifying all pcaps.

4 Examination

Examine the data involves assessing and extracting the relevant pieces of information from the collected data. This phase may also involve bypassing or mitigating OS or application features that obscure data and code, such as data compression, encryption, and access control mechanisms. An acquired hard drive may contain hundreds of thousands of data files; identifying the data files that contain information of interest, including information concealed through file compression and access control.
There're Various tools and techniques can be used to reduce the amount of data that has to be sifted through. Text and pattern searches can be used to identify pertinent data, such as finding documents that mention a particular subject or person, or identifying e-mail log entries for a particular e-mail address.

4.1 Methodology

The analysis analysed the contents using network forensic tools such as Wireshark,tshark, coreutils executing under Windows 7 Enterprise SP1 on AMD Athlon X2 and 4 Gb of RAM, also a Debian Gnu/Linux under Virtualbox on 750 Mb RAM.

5 Analysis

The analyst should study and analyze the data to draw conclusions from it.The foundation of forensics is using a methodical approach to reach appropriate conclusions based on the available data or determine that no conclusion can yet be drawn. The analysis should include identifying people, places, items, and events, and determining how these elements are related so that a conclusion can be reached. Often, this effort will include correlating data among multiple sources or files.

5.1 Network Capture CAPTURA1.:

5.1.1 CAPTURA1.cap

The PCAP network capture or packet capture file CAPTURE1.pcap has the forensic parameters as given below. The evidence for these details is provided in Figure 1 extracted from Wireshark Ver 1.10.2 (SVN Rev 51934 from /trunk-1.10):
Summary created by Wireshark (SVN Rev 51934 from /trunk-1.10)
File:
Name: C:/c1b3r/RetoForense/sPacketCapturesM - copia/**CAPTURA1.pcap**
Length: 20169170 bytes
Format: Wireshark/... - pcapng
Encapsulation: Ethernet
Time:
First packet: **2012-11-27 10:15:24**
Last packet: **2012-11-27 10:27:20**
Elapsed: 00:11:55
Capture:
OS: **32-bit Windows 7, build 7600**
Capture application: Dumpcap 1.8.2 (SVN Rev 44520 from /trunk-1.8)
Dropped packets: unknown
Capture filter: none
Link type: Ethernet
Packet size limit 65535 bytes

5.1.2 Network Components Identified

Based on the statistics report, it appears that the devices Destination: Cisco-Li-0c-7b-9c and MS-NLB-PhysServer-12-29-96-13-be were significantly involved in the conversations tracked on the network capture file and contains details of the investigation.

Address A	Address B	Packets
Cisco-Li_0c:7b:9c	MS-NLB-PhysServer-12_29:96:13:be	26 274
MS-NLB-PhysServer-12_29:96:13:be	Apple_92:6e:3d	619
MS-NLB-PhysServer-12_29:96:13:be	f4:b1:d3:ba:a1:17	282
MS-NLB-PhysServer-12_29:96:13:be	Broadcast	41
IPv4mcast_00:00:fc	MS-NLB-PhysServer-12_29:96:13:be	16

Network Components.

5.1.3 Details CAPTURA1:

We could refer to access.log to check what was accesed during the connection, I've used wireshark to open CAPTURA1.cap ,the first thing to notice here is packet 1 had an arrival time: **Nov 27, 2012 10:15:24.871592000 Hora est. Pacífico, Sudamérica** the details of time will let me to create a chronology of the data, and it was from Sudamérica thats what the challenge say,mainly the ip source is *192.168.0.57* so I'm going to suposse that this is client machine with mac address *02:0c:29:96:13:be.*

understanding the question they're asking us for specific filenames with singular hashes.

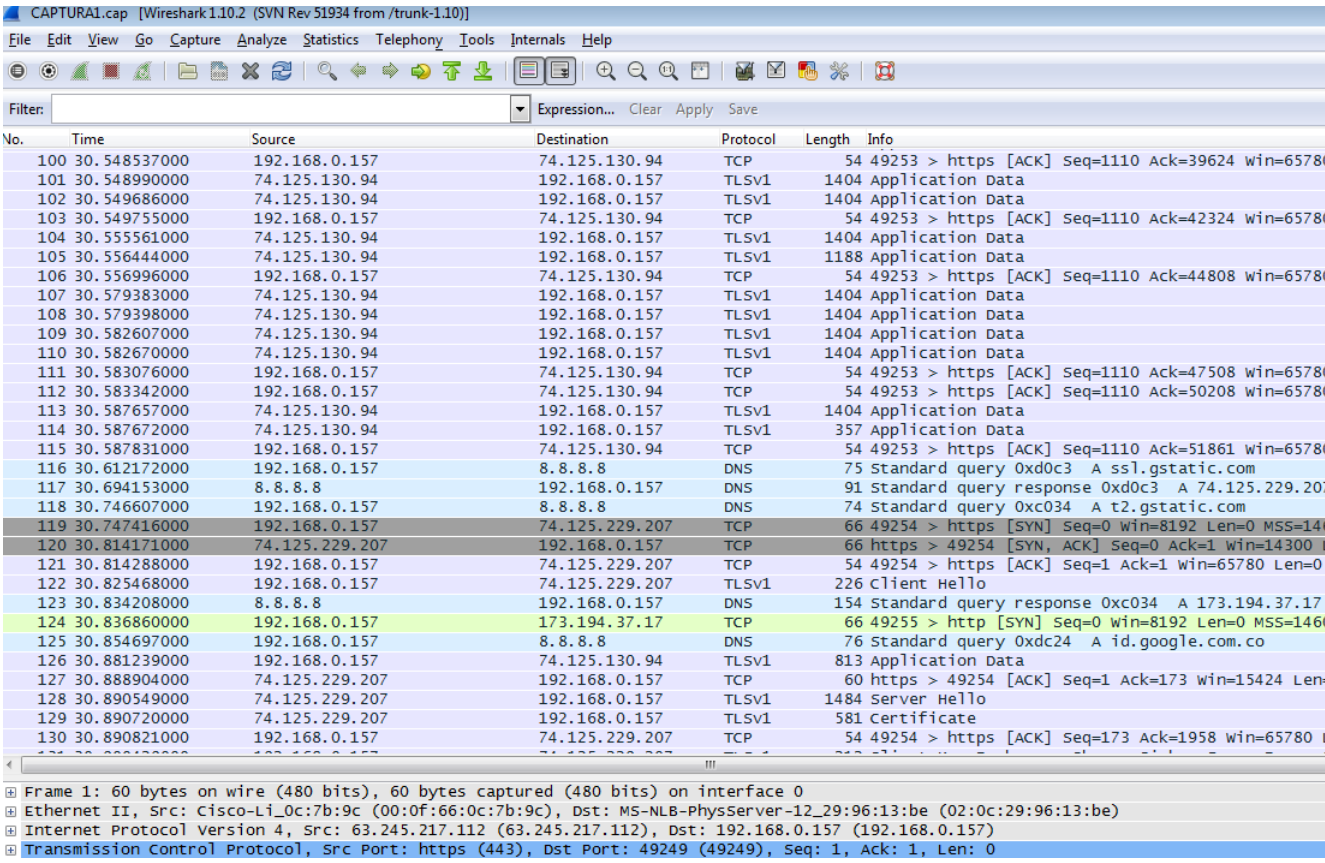


Figure 2:Opening the packet capture.

Keeping that in mind we have diferent options:

- File Carving with Foremost or other similar tools.
- Use the same wireshark to extract files in the packet capture.

My choice was use the same wireshark to extract the files, to do this we only need to read the packets and filter the info column to see alot of get request.we can recover the files as is shown in Figure 5 :

No.	Time	Source	Destination	Protocol	Length	Info
27042	652.373436000	192.168.0.157	69.171.228.74	TLSv1	81	Encrypted Alert
27049	652.534404000	69.171.228.74	192.168.0.157	TLSv1	81	Encrypted Alert
27072	660.922666000	192.168.0.157	74.125.229.228	TLSv1	81	Encrypted Alert
773	80.307444000	192.168.0.157	79.125.109.24	HTTP	459	GET / HTTP/1.1
1282	89.599682000	192.168.0.157	79.125.109.24	HTTP	359	GET / HTTP/1.1
2508	94.347045000	192.168.0.157	67.205.51.26	HTTP	546	GET / HTTP/1.1
4184	99.127906000	192.168.0.157	79.125.109.24	HTTP	595	GET / HTTP/1.1
5833	129.776424000	192.168.0.157	74.125.130.106	HTTP	748	GET / HTTP/1.1
5845	129.911709000	192.168.0.157	74.125.130.94	HTTP	751	GET / HTTP/1.1
7263	161.835516000	192.168.0.157	216.200.20.161	HTTP	554	GET / HTTP/1.1
11918	370.286158000	192.168.0.157	174.137.42.75	HTTP	552	GET / HTTP/1.1
20794	551.204318000	192.168.0.157	173.194.37.10	HTTP	362	GET / HTTP/1.1
26323	630.327931000	192.168.0.157	173.194.37.0	HTTP	484	GET /-0hLf6ZziRLs/T5jYMLRdBSI/AAAAAAAACNo/LuC90dTzhxQ/s320/imagen9.jpg
21494	553.472691000	192.168.0.157	173.194.37.6	HTTP	432	GET /-1tITUueIsYo/UH2SzvDKXLI/AAAAAAAACSQ/OPXRYpjUZb8/s200/foto12.jpg
21040	552.368335000	192.168.0.157	173.194.37.8	HTTP	432	GET /-3MdG3uUJn2w/UH2SvdlO-EI/AAAAAAAACSI/xDeGvkdLCdc/s200/foto10.jpg
21300	553.072349000	192.168.0.157	173.194.37.0	HTTP	432	GET /-3dGN6ykKHJ4/UH2SgwYHLvI/AAAAAAAACSg/HFYqLj7UI2Q/s200/foto14.jpg
21361	553.232440000	192.168.0.157	173.194.37.6	HTTP	431	GET /-4LoIZkP1n2Q/UH2UDnmPUrI/AAAAAAAACTc/TexVrx8SEBU/s200/foto1.JPG H
26315	630.325331000	192.168.0.157	173.194.37.2	HTTP	484	GET /-5ykt580LtTI/T5jVqvPc2DI/AAAAAAAACMY/QUOX9wB1MiQ/s320/imagen1.jpg
20977	552.251195000	192.168.0.157	173.194.37.6	HTTP	438	GET /-68Qj83AgFxQ/UH2YuOOe5rI/AAAAAAAACVE/uQbF2fi-MyA/s200/an8as8a8ns8
26321	630.326626000	192.168.0.157	173.194.37.0	HTTP	484	GET /-6bxRPSst8PA/T5jXQ2sxdaI/AAAAAAAACNI/FhDwt2L3PQs/s320/imagen7.jpg
20911	552.187552000	192.168.0.157	173.194.37.8	HTTP	431	GET /-8_vPovzxTjo/UH2URf7o8qI/AAAAAAAACTk/ZUnJAO-vtCk/s200/foto2.JPG H
20924	552.191972000	192.168.0.157	173.194.37.0	HTTP	431	GET /-9R0ePnCHNH4/UH2Ufbm-AvI/AAAAAAAACTw/Or-y14g01Es/s200/foto3.JPG H
25700	607.429227000	192.168.0.157	173.194.37.6	HTTP	456	GET /-BwlMTQTMD-Q/TidqlEXPU2I/AAAAAAAACJQ/6fJCoWTkSqw/s320/HoneyNets.j
26326	630.328923000	192.168.0.157	173.194.37.2	HTTP	485	GET /-EvT-N93iXOk/T5jZfsNpInI/AAAAAAAACOA/7H6LBkqKgXM/s320/imagen12.jp
26333	630.331316000	192.168.0.157	173.194.37.2	HTTP	485	GET /-F1G9DzY-hRo/T5jbk_7T19I/AAAAAAAACOg/dmDnKwCJtT8/s320/imagen16.jp
26320	630.326454000	192.168.0.157	173.194.37.6	HTTP	484	GET /-IOBREyCjXiO/T5jW-67_U1I/AAAAAAAACNA/OmmxsLGPXoQ/s320/imagen6.jpg
20969	552.248553000	192.168.0.157	173.194.37.2	HTTP	432	GET /-K2k5kXeusS4/UH2SzSnts1I/AAAAAAAACTI/XQEckTWwhUI/s200/foto21.jpg
20896	552.174756000	192.168.0.157	173.194.37.8	HTTP	443	GET /-KZMk3zGtnAw/UJgkIOXw5-I/AAAAAAAACXs/Ysskx2ow4VY/s1600/networkFor
20971	552.249181000	192.168.0.157	173.194.37.2	HTTP	432	GET /-KeU2OzgBlYc/UH2SkBqOasI/AAAAAAAACSo/kPhqFos5HSQ/s200/foto16.jpg
20925	552.192679000	192.168.0.157	173.194.37.0	HTTP	432	GET /-N4CEitI8ucs/UH2SobUDHFI/AAAAAAAACSw/kOW1LwozPh0/s200/foto18.jpg
26331	630.330614000	192.168.0.157	173.194.37.2	HTTP	523	GET /-NT4Rl_COlcA/T5jo6wjjzTI/AAAAAAAACPo/x_T1cJXyPdo/s1600/Captura+de
26327	630.329222000	192.168.0.157	173.194.37.8	HTTP	485	GET /-PO1h4WbpuO0/T5jc2ool64I/AAAAAAAACOw/GwHCzJcVxws/s320/imagen18.jp
26314	630.325075000	192.168.0.157	173.194.37.2	HTTP	500	GET /-RCV-K-DNlo8/T5jdOFIU68I/AAAAAAAACO4/bpsBadkNVvQ/s320/banner-serv
20972	552.249459000	192.168.0.157	173.194.37.2	HTTP	450	GET /-RCV-K-DNlo8/T5jdOFIU68I/AAAAAAAACO4/bpsBadkNVvQ/s72-c/banner-ser
20912	552.188604000	192.168.0.157	173.194.37.0	HTTP	441	GET /-RJy9rphnuM8/UJIOj9LtuqI/AAAAAAAACWQ/-rfX7qWvQBU/s400/Misconfv1Cl
26322	630.326797000	192.168.0.157	173.194.37.8	HTTP	484	GET /-RbGzIuNkye4/T5jXy5HDagI/AAAAAAAACNg/LX6SoREkOSc/s320/imagen8.jpg
20908	552.180717000	192.168.0.157	173.194.37.8	HTTP	433	GET /-RyURWoq2RMI/UH2YEy9ApaI/AAAAAAAACU8/ksv1Hv25YCc/s200/nonroot.JPG
26334	630.331610000	192.168.0.157	173.194.37.6	HTTP	485	GET /-SPrl3-v3zRw/T5jbwUBTA7I/AAAAAAAACOo/_hjldLySLzA/s320/imagen17.jp
26325	630.328619000	192.168.0.157	173.194.37.8	HTTP	485	GET /-UnmChhJGGYc/T5jY6twPAOI/AAAAAAAACNw/9GkSmolOkiE/s320/imagen10.jp
26332	630.330998000	192.168.0.157	173.194.37.0	HTTP	522	GET /-Y-c_5edD_yE/T5jn8PSFdXI/AAAAAAAACPY/O52HnW_t5Mg/s320/Captura+de+
26329	630.329822000	192.168.0.157	173.194.37.0	HTTP	485	GET /-Y36dpgYw5Kg/T5jadXCBBKI/AAAAAAAACOQ/m3mFVrP63yw/s320/imagen14.jp
20906	552.179368000	192.168.0.157	173.194.37.8	HTTP	434	GET /-Z99QxoJiaoM/UH3T2xBsN6I/AAAAAAAACVw/pZjpIRVS_G4/s400/imagen24.jp
20976	552.250906000	192.168.0.157	173.194.37.6	HTTP	431	GET /-b61RtwazPKM/UH2VbPRF2_I/AAAAAAAACUc/PHhwYOD9dAw/s320/foto8.JPG H

Figure 3:Filter using Column Info.

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
15602	487.900434000	69.31.72.34	192.168.0.157	HTTP	687	HTTP/1.1 200 OK (application/x-javascript)
15616	487.961469000	69.31.72.34	192.168.0.157	HTTP	1495	HTTP/1.1 200 OK (application/x-javascript)
15662	488.136267000	69.31.72.34	192.168.0.157	HTTP	695	HTTP/1.1 200 OK (application/x-javascript)
15669	488.194768000	69.31.72.34	192.168.0.157	HTTP	972	HTTP/1.1 200 OK (application/x-javascript)
16535	499.671386000	173.192.170.82	192.168.0.157	HTTP	1497	HTTP/1.1 200 OK (application/x-javascript)
16540	499.676130000	173.192.170.82	192.168.0.157	HTTP	577	HTTP/1.1 200 OK (application/x-javascript)
17288	501.501348000	192.204.4.73	192.168.0.157	HTTP	956	HTTP/1.1 200 OK (application/x-javascript)
17738	502.494896000	23.62.207.139	192.168.0.157	HTTP	152	HTTP/1.1 200 OK (application/x-javascript)
19644	514.661510000	69.31.72.34	192.168.0.157	HTTP	1274	HTTP/1.1 200 OK (application/x-javascript)
20216	531.940023000	23.62.207.139	192.168.0.157	HTTP	878	HTTP/1.1 200 OK (application/x-javascript)
20660	537.874297000	69.31.72.34	192.168.0.157	HTTP	222	HTTP/1.1 200 OK (application/x-javascript)
17658	502.264182000	80.237.211.10	192.168.0.157	HTTP	443	HTTP/1.1 200 OK (application/x-shockwave-flash)
17853	502.755191000	173.192.170.82	192.168.0.157	HTTP	160	HTTP/1.1 200 OK (application/x-shockwave-flash)
19111	505.894316000	94.249.188.201	192.168.0.157	HTTP	1513	HTTP/1.1 200 OK (application/x-shockwave-flash)
22180	556.452765000	74.125.137.95	192.168.0.157	HTTP	790	HTTP/1.1 200 OK (application/x-shockwave-flash)
11655	339.909428000	192.168.0.159	192.168.0.157	HTTP	1454	HTTP/1.1 200 OK (application/zip)
12381	373.058391000	192.168.0.159	192.168.0.157	HTTP	1511	HTTP/1.1 200 OK (application/zip)
27036	650.071761000	192.168.0.159	192.168.0.157	HTTP	1374	HTTP/1.1 200 OK (application/zip)
1731	90.978568000	173.194.37.140	192.168.0.157	HTTP	363	HTTP/1.1 200 OK (font/woff)
2447	94.053464000	79.125.109.24	192.168.0.157	HTTP	695	HTTP/1.1 200 OK (image/jpeg)
8501	166.143018000	216.200.20.161	192.168.0.157	HTTP	1490	HTTP/1.1 200 OK (image/jpeg)
13170	414.195784000	208.70.196.59	192.168.0.157	HTTP	1016	HTTP/1.1 200 OK (image/jpeg)
13288	414.493623000	208.70.196.59	192.168.0.157	HTTP	726	HTTP/1.1 200 OK (image/jpeg)
13337	414.602728000	208.70.196.59	192.168.0.157	HTTP	960	HTTP/1.1 200 OK (image/jpeg)
13350	414.670017000	208.70.196.59	192.168.0.157	HTTP	1412	HTTP/1.1 200 OK (image/jpeg)
13366	414.701704000	208.70.196.59	192.168.0.157	HTTP	1302	HTTP/1.1 200 OK (image/jpeg)
13389	414.855049000	208.70.196.59	192.168.0.157	HTTP	1139	HTTP/1.1 200 OK (image/jpeg)
13456	415.108132000	208.70.196.59	192.168.0.157	HTTP	1065	HTTP/1.1 200 OK (image/jpeg)
13468	415.155160000	208.70.196.59	192.168.0.157	HTTP	370	HTTP/1.1 200 OK (image/jpeg)
13472	415.277339000	208.70.196.59	192.168.0.157	HTTP	526	HTTP/1.1 200 OK (image/jpeg)
13495	415.497952000	208.70.196.59	192.168.0.157	HTTP	63	HTTP/1.1 200 OK (image/jpeg)
13551	415.728341000	208.70.196.59	192.168.0.157	HTTP	127	HTTP/1.1 200 OK (image/jpeg)
13553	415.728375000	208.70.196.59	192.168.0.157	HTTP	1081	HTTP/1.1 200 OK (image/jpeg)
13609	415.928131000	208.70.196.59	192.168.0.157	HTTP	421	HTTP/1.1 200 OK (image/jpeg)
13612	415.929113000	208.70.196.59	192.168.0.157	HTTP	1347	HTTP/1.1 200 OK (image/jpeg)
13617	415.936015000	208.70.196.59	192.168.0.157	HTTP	286	HTTP/1.1 200 OK (image/jpeg)
13687	417.804462000	208.70.196.59	192.168.0.157	HTTP	1513	HTTP/1.1 200 OK (image/jpeg)
15833	490.182523000	74.125.229.249	192.168.0.157	HTTP	856	HTTP/1.1 200 OK (image/jpeg)
479	46.037454000	74.125.130.94	192.168.0.157	HTTP	88	HTTP/1.1 200 OK (image/x-icon)
664	49.367564000	194.9.95.191	192.168.0.157	HTTP	1272	HTTP/1.1 200 OK (image/x-icon)

Figure 4:Received Files.

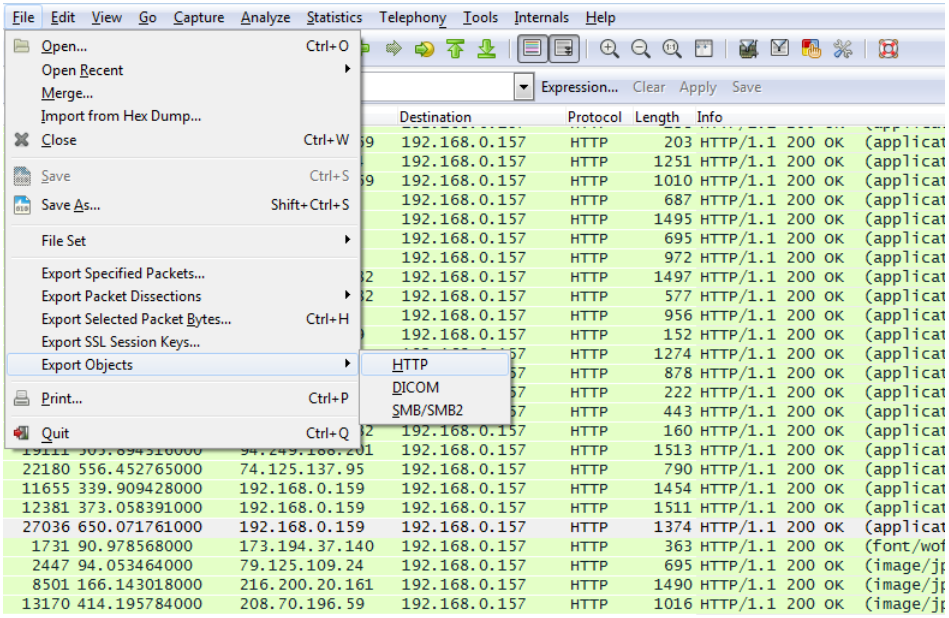


Figure 5:File, Export Objects, Http.

Now we got up all the files exactly 957 elements also identifying the hash **42c97d472146510bd1a8f183ea0ef56ee8309** using Hash iD:
Possible Hashs:
[+] SHA-1
[+] MySQL5 - SHA-1(SHA-1($pass))
Sha1sum utility will be ok for this task, first create recursively sha1 hashes from all files in required directory,after I grep the output with **grep Â42c97**

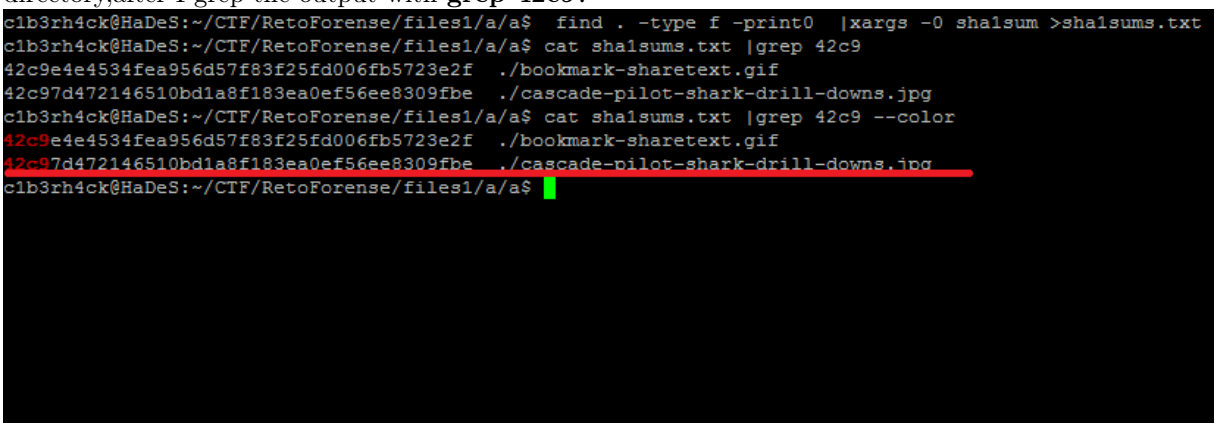


Figure 6:Recursively Sha1sum all files.

42c97d472146510bd1a8f183ea0ef56ee8309fbe ./cascade-pilot-shark-drill-downs.jpg
89ded89ce3ee7698e7da974e025db612374d4264 ./0alsa00asl3.odt
eef4c1d9ee68bbd937f8681ccc5e93b8119d0f79 ./Evidencia(2).zip
eef4c1d9ee68bbd937f8681ccc5e93b8119d0f79 ./Evidencia(1).zip
eef4c1d9ee68bbd937f8681ccc5e93b8119d0f79 ./Evidencia.zip
Now we know the files let me go more deeper,I've found in the get request the main conversation between **192.168.0.157** and **192.168.0.159**I used the next filter :

(ip.src==192.168.0.157)&& (ip.dst==192.168.0.159)

The files of the task correspond to the next packet capture numbers:

Filename	Packet Number
Evidencia.zip	11579
Evidencia(1).zip	12307
Evidencia(2).zip	26956
0alsa00asl3.odt	10664
cascade-pilot-shark-drill-downs.jpg	13171

The testimony given by the witness about the date can't be confirmed meanwhile he says :
Información adicional: Según el testigo principal, los hechos ocurrieron el ***Miércoles 28 de Noviembre de 2012 a partir de las 17:20 en Sydney, Australia.***

I used different filters in wireshark but without any result of the given date.

(frame.time == "Nov 28, 2012 17:20:00") || (frame.time ge "Nov 28, 2012 17:20:00")
http.date== "Thur, 28 Nov 2013 17:20:00 GMT+11"
http.date== "Thur, 28 Nov 2013 17:20:00 "

I've verified what urls had the first pcap file using **tshark -R http.host -Tfields -e http.host -r CAPTURA1.cap |sort | uniq -c | sort -nr** and we obtains:

```
103 www.xplico.org
 96 neobits.org
 87 www.riverbed.com
 60 eforensicsmag.com
 53 www.netwitness.com
 33 ws.cf.wireshark.net
 33 2.bp.blogspot.com
 31 www.google-analytics.com
 29 www.netresec.com
 29 4.bp.blogspot.com
 24 3.bp.blogspot.com
 22 www.blogger.com
 22 1.bp.blogspot.com
 21 casidiablo.net
 18 192.168.0.159
 14 www.google.com.co
 14 static.ak.fbcdn.net
 13 www.blogblog.com
 12 www.python.org
 12 1.gravatar.com
 11 www.wireshark.org
 10 pagead2.googlesyndication.com
```

Figure 7:Urls inside Packet capture.

5.2 Network Capture *CAPTURA2A-CAPTURA2B*

5.2.1 CAPTURA2A.pcap

Summary created by Wireshark (SVN Rev 51934 from /trunk-1.10)
File:
Name: C:/c1b3r/RetoForense/sPacketCapturesM - copia/CAPTURA2A.pcap
Length: 271624 bytes
Format: Wireshark/tcpdump/... - pcap
Encapsulation: Ethernet
Time:
First packet: **2012-11-29 21:50:15**
Last packet: **2012-11-29 21:51:58**
Elapsed: 00:01:43
Capture:
OS: **32-bit Windows 7, build 7600**
Capture application: Dumpcap 1.8.2 (SVN Rev 44520 from /trunk-1.8)
Dropped packets: unknown
Capture filter: unknown
Link type: Ethernet
Packet size limit 65535 bytes
Statistics:
Packets: 2199
Between first and last packet:103,366 sec
Avg. packets/sec: 21,274

Avg packet size: 107,511 bytes
Bytes: 236416
Avg bytes/sec: 2287,178
Avg Mbit/sec: 0,018

5.2.2 CAPTURA2B.pcap

Summary created by Wireshark (SVN Rev 51934 from /trunk-1.10)
File:
Name: C:/c1b3r/RetoForense/sPacketCapturesM - copia/CAPTURA2B.pcap
Length: 872848 bytes
Format: Wireshark/... - pcapng
Encapsulation: Ethernet
Time:
First packet: : **2012-11-29 21:50:11**
Last packet: **2012-11-29 21:52:04**
Elapsed: 00:01:52
Capture:
OS: **Mac OS 10.6.8 (Darwin 10.8.0)**
Capture application: Dumpcap 1.8.2 (SVN Rev 44520 from /trunk-1.8)
Dropped packets: 0 (0,000%)
Capture filter: none
Link type: Ethernet
Packet size limit 65535 bytes
Statistics:
Packets: 2224
Between first and last packet:112,414 sec
Avg. packets/sec: 19,784
Avg packet size: 358,853 bytes
Bytes: 798089
Avg bytes/sec: 7099,525
Avg Mbit/sec: 0,057

5.2.3 Network Components Identified

There are a couple of things to notice here, the time between network capture A and network capture B has a small difference when the first packet was captured *"21:50:15", "21:50:11"*.

So lets start with CAPTURA2A.pcap in this pcap I can see lots of differents request between them echo ping request, Dropbox Lan sync, Http, Dns, Dhcp and others, we need to identify the player in this capture, it can be done easily using wireshark : statistic - conversations.

Apple_0e:bb:60	Broadcast
Trendnet_cf:8c:04	Apple_19:0c:b7
IPv4mcast_00:00:fb	Apple_19:0c:b7
IPv6mcast_00:00:00:fb	Apple_19:0c:b7
Apple_19:0c:b7	Broadcast

Figure 8:Network Components .

In figure 8 shows there is 2 apple devices,checking for the conversations between ips we can figure out the most active was 192.168.10.99 to 192.168.10.100.

IPv4 Conversations

Address A	Address B	Packets	Bytes	Packets A→B	Bytes A→B	Packets A←B	Byt
0.0.0.0	255.255.255.255	17	5 814	17	5 814	0	
192.168.10.99	192.168.10.100	2 148	223 948	2 148	223 948	0	
169.254.185.91	224.0.0.251	6	1 872	6	1 872	0	
169.254.203.207	169.254.255.255	15	2 792	15	2 792	0	
169.254.203.207	255.255.255.255	3	612	3	612	0	
169.254.185.91	255.255.255.255	5	570	5	570	0	

Figure 9:Ipv4 Conversations,under statistics tab from CAPTURA2A.pcap.

Filtering this conversation I got a few user and passwords :

- root:non
- nonroot:nonroot
- admin:nonroot
- **admin:clavesupersegura**

34	33.473580	192.168.10.99	192.168.10.100	HTTP	371	GET / HTTP/1.1
44	38.287790	192.168.10.99	192.168.10.100	HTTP	406	GET / HTTP/1.1
54	43.450470	192.168.10.99	192.168.10.100	HTTP	414	GET / HTTP/1.1
58	43.451157	192.168.10.99	192.168.10.100	HTTP	414	GET / HTTP/1.1
67	48.294026	192.168.10.99	192.168.10.100	HTTP	414	GET / HTTP/1.1
71	48.294797	192.168.10.99	192.168.10.100	HTTP	414	GET / HTTP/1.1
83	53.551404	192.168.10.99	192.168.10.100	HTTP	426	GET / HTTP/1.1
87	53.552781	192.168.10.99	192.168.10.100	HTTP	426	GET / HTTP/1.1

Figure 10:Packets for users and passwords.

admin:clavesupersegura is the user and password for admin access, a router or network device,maybe zte-ac30-web based on the results of google intitle:"/wireless/opmode.asp".
In packet 1833 post request stablish the passphrase for the wireless access as is show below.
`rebootNeeded=no&ssidIndex=0&security_mode=WPAPSK&security_shared_mode=WEP\\ &wep_default_key=1&wep`
`&wep_key_3=&WEP3Select=0&wep_key_4=&WEP4Select=0&cipher=0 &passphrase=seczone2012&keyRenew`

passphrase=seczone2012

That was interesting, multiple access to the admin router panel so we need to check the second capture again identifying the main players and compare the differences with CAPTURA2A.

Address A	Address B	Packets	Bytes	Packets A→B	Bytes A→B	Packets A←B	Bytes A←B
192.168.10.99	192.168.10.100	2 068	753 421	0	0	2 068	753 421
192.168.10.100	239.255.255.250	76	31 248	76	31 248	0	0
0.0.0.0	255.255.255.255	26	8 892	26	8 892	0	0

Figure 11:Ipv4 Conversations,CAPTURA2B.pcap.

There is a difference in packets and Bytes in CAPTURA2B we have more activity here,and the ssid of the Access point is NONROOT-AP, Logging Failed Log-in Attempts can be see in packet number 63, 87, 118, they're trying to access the wireless access point that it is `http://www.trendnet.com/langsp/products/proddetail.asp?prod=140_TEW-638APB` TEW-638APB not as we tought zte-ac30-web, this can be confirmed in packet number 139 following the tcp streaming in title html .default ssid for ap is .var **SSID = '50495a4152524f'**
There is another interesting thing in packet 1809

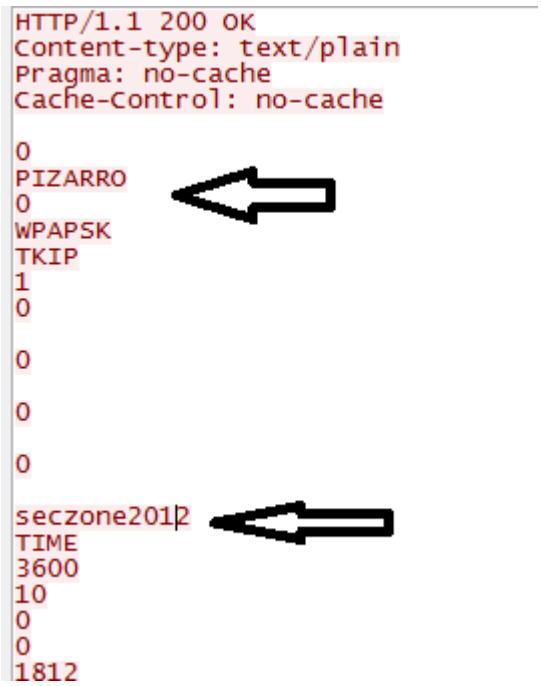


Figure 12:Passwords for wifi network.

4. ¿Cuántas peticiones de ping se realizaron?
Doing a task like that can be simple using tshark:

tshark -r CAPTURA1.cap -R icmp -T fields -e frame.number|wc -l 145
tshark -r CAPTURA2A.cap -R icmp -T fields -e frame.number|wc -l 13
tshark -r CAPTURA2B.cap -R icmp -T fields -e frame.number|wc -l 13
tshark -r CAPTURA4.cap -R icmp -T fields -e frame.number|wc -l 30
Total icmp echo reply:201

The command above simple said -r to open the capture packet, -R Cause the specified filter in this case icmp, -T Set the format of the output fields specified with the -e frame number,pipe let you use the output of a program as the input of another one in this case I counted the numbers of frames with correspond to icmp, you can see more information of tshark in this website

5.3 Network Capture *CAPTURA3A-CAPTURA3B*

5.3.1 CAPTURA3A.cap

Summary created by Wireshark (SVN Rev 51934 from /trunk-1.10)
File:
Name: C:/c1b3r/RetoForense/sPacketCapturesM - copia/CAPTURA3A.cap
Length: 61243 bytes
Format: Wireshark/tcpdump/... - pcap
Encapsulation: IEEE 802.11 Wireless LAN
Time:
First packet: **2012-11-29 20:15:57**
Last packet: **2012-11-29 20:16:36**
Elapsed: 00:00:39
Capture:
Unknown interface:
Capture application: Dumpcap 1.8.2 (SVN Rev 44520 from /trunk-1.8)
Dropped packets: unknown
Capture filter: unknown
Link type: IEEE 802.11 Wireless LAN
Packet size limit 65535 bytes
Statistics:
Packets: 701
Between first and last packet:39,624 sec

Avg. packets/sec: 17,691
Avg packet size: 71,331 bytes
Bytes: 50003
Avg bytes/sec: 1261,950
Avg Mbit/sec: 0,010

5.3.2 CAPTURA3B.cap

Summary created by Wireshark (SVN Rev 51934 from /trunk-1.10)
File:
Name: C:/c1b3r/RetoForense/sPacketCapturesM - copia/CAPTURA3B.cap
Length: 340554 bytes
Format: Wireshark/tcpdump/... - pcap
Encapsulation: IEEE 802.11 Wireless LAN
Time:
First packet: **2012-11-29 20:16:43**
Last packet: **2012-11-29 20:18:21**
Elapsed: 00:01:37
Capture:
Unknown interface:
Dropped packets: unknown
Capture filter: unknown
Link type: IEEE 802.11 Wireless LAN
Packet size limit 65535 bytes
Statistics:
Packets: 2217
Between first and last packet:97,475 sec
Avg. packets/sec: 22,744
Avg packet size: 137,599 bytes
Bytes: 305058
Avg bytes/sec: 3129,611
Avg Mbit/sec: 0,025
Note [1]

5.3.3 Details CAPTURA3A-3B:

I analyzed the network traffic in this, with have a Wifi network, and I noticed a remarkable amount of 802.11 deauth packets. we don't know where the attack came from and also you cannot stop a bad guy from sending deauthentication packets it is due to the role model of wifi design.send deauth packets is that this helps them execute a dictionary attack against your passphrase. If a bad guy captures a copy of the initial handshake, they can try out various guesses at your passphrase and test whether they are correct. Sending a deauth packet forces the targeted device to disconnect and reconnect, allowing an eavesdropper to capture a copy of the initial handshake. This can be confirmed in the figure 13.
We can identify the ssid `"PIZARRO"` and the client connect to it Apple-92:6e:3d the victim for aireplay deauthentication attack against the network.

[1]"Computed Hashes refer to Figure 1"

	Time	Source	Destination	Protocol	Info
77	3.397804	Apple_92:6e:3d	Trendnet_cf:8c:04	802.11	Deauthentication, SN=1, FN=0, Flags=.....
79	3.400424	Apple_92:6e:3d	Trendnet_cf:8c:04	802.11	Deauthentication, SN=1, FN=0, Flags=.....
99	3.425512	Trendnet_cf:8c:04	Apple_92:6e:3d	802.11	Deauthentication, SN=10, FN=0, Flags=.....
101	3.427560	Trendnet_cf:8c:04	Apple_92:6e:3d	802.11	Deauthentication, SN=10, FN=0, Flags=.....
309	3.692776	Trendnet_cf:8c:04	Apple_92:6e:3d	802.11	Deauthentication, SN=100, FN=0, Flags=.....
311	3.695336	Trendnet_cf:8c:04	Apple_92:6e:3d	802.11	Deauthentication, SN=100, FN=0, Flags=.....
312	3.695336	Apple_92:6e:3d	Trendnet_cf:8c:04	802.11	Deauthentication, SN=101, FN=0, Flags=.....
314	3.697384	Apple_92:6e:3d	Trendnet_cf:8c:04	802.11	Deauthentication, SN=101, FN=0, Flags=.....
315	3.698920	Trendnet_cf:8c:04	Apple_92:6e:3d	802.11	Deauthentication, SN=102, FN=0, Flags=.....
317	3.700456	Trendnet_cf:8c:04	Apple_92:6e:3d	802.11	Deauthentication, SN=102, FN=0, Flags=.....
318	3.701480	Apple_92:6e:3d	Trendnet_cf:8c:04	802.11	Deauthentication, SN=103, FN=0, Flags=.....
320	3.703528	Apple_92:6e:3d	Trendnet_cf:8c:04	802.11	Deauthentication, SN=103, FN=0, Flags=.....
321	3.705064	Trendnet_cf:8c:04	Apple_92:6e:3d	802.11	Deauthentication, SN=104, FN=0, Flags=.....
323	3.706600	Trendnet_cf:8c:04	Apple_92:6e:3d	802.11	Deauthentication, SN=104, FN=0, Flags=.....
324	3.707112	Apple_92:6e:3d	Trendnet_cf:8c:04	802.11	Deauthentication, SN=105, FN=0, Flags=.....
325	3.709160	Apple_92:6e:3d	Trendnet_cf:8c:04	802.11	Deauthentication, SN=105, FN=0, Flags=.....
326	3.710696	Trendnet_cf:8c:04	Apple_92:6e:3d	802.11	Deauthentication, SN=106, FN=0, Flags=.....
329	3.713768	Trendnet_cf:8c:04	Apple_92:6e:3d	802.11	Deauthentication, SN=106, FN=0, Flags=.....
328	3.712744	Apple_92:6e:3d	Trendnet_cf:8c:04	802.11	Deauthentication, SN=107, FN=0, Flags=.....
330	3.713768	Apple_92:6e:3d	Trendnet_cf:8c:04	802.11	Deauthentication, SN=107, FN=0, Flags=.....
332	3.716840	Trendnet_cf:8c:04	Apple_92:6e:3d	802.11	Deauthentication, SN=108, FN=0, Flags=.....
334	3.718888	Trendnet_cf:8c:04	Apple_92:6e:3d	802.11	Deauthentication, SN=108, FN=0, Flags=.....
335	3.718888	Apple_92:6e:3d	Trendnet_cf:8c:04	802.11	Deauthentication, SN=109, FN=0, Flags=.....
336	3.720936	Apple_92:6e:3d	Trendnet_cf:8c:04	802.11	Deauthentication, SN=109, FN=0, Flags=.....
100	3.427560	Apple_92:6e:3d	Trendnet_cf:8c:04	802.11	Deauthentication, SN=11, FN=0, Flags=.....
102	3.430632	Apple_92:6e:3d	Trendnet_cf:8c:04	802.11	Deauthentication, SN=11, FN=0, Flags=.....
337	3.722472	Trendnet_cf:8c:04	Apple_92:6e:3d	802.11	Deauthentication, SN=110, FN=0, Flags=.....
338	3.724008	Trendnet_cf:8c:04	Apple_92:6e:3d	802.11	Deauthentication, SN=110, FN=0, Flags=.....
339	3.725544	Apple_92:6e:3d	Trendnet_cf:8c:04	802.11	Deauthentication, SN=111, FN=0, Flags=.....
340	3.727592	Apple_92:6e:3d	Trendnet_cf:8c:04	802.11	Deauthentication, SN=111, FN=0, Flags=.....
341	3.729128	Trendnet_cf:8c:04	Apple_92:6e:3d	802.11	Deauthentication, SN=112, FN=0, Flags=.....
343	3.732200	Trendnet_cf:8c:04	Apple_92:6e:3d	802.11	Deauthentication, SN=112, FN=0, Flags=.....
342	3.731688	Apple_92:6e:3d	Trendnet_cf:8c:04	802.11	Deauthentication, SN=113, FN=0, Flags=.....
344	3.732200	Apple_92:6e:3d	Trendnet_cf:8c:04	802.11	Deauthentication, SN=113, FN=0, Flags=.....
345	3.735272	Trendnet_cf:8c:04	Apple_92:6e:3d	802.11	Deauthentication, SN=114, FN=0, Flags=.....
347	3.737832	Trendnet_cf:8c:04	Apple_92:6e:3d	802.11	Deauthentication, SN=114, FN=0, Flags=.....
346	3.737832	Apple_92:6e:3d	Trendnet_cf:8c:04	802.11	Deauthentication, SN=115, FN=0, Flags=.....
348	3.739880	Apple_92:6e:3d	Trendnet_cf:8c:04	802.11	Deauthentication, SN=115, FN=0, Flags=.....
349	3.740904	Trendnet_cf:8c:04	Apple_92:6e:3d	802.11	Deauthentication, SN=116, FN=0, Flags=.....
351	3.743464	Trendnet_cf:8c:04	Apple_92:6e:3d	802.11	Deauthentication, SN=116, FN=0, Flags=.....
350	3.743464	Apple_92:6e:3d	Trendnet_cf:8c:04	802.11	Deauthentication, SN=117, FN=0, Flags=.....
352	3.743976	Apple_92:6e:3d	Trendnet_cf:8c:04	802.11	Deauthentication, SN=117, FN=0, Flags=.....
354	3.747048	Trendnet_cf:8c:04	Apple_92:6e:3d	802.11	Deauthentication, SN=118, FN=0, Flags=.....
356	3.749608	Trendnet_cf:8c:04	Apple_92:6e:3d	802.11	Deauthentication, SN=118, FN=0, Flags=.....

Figure 13:Deauthentication notification.

48.135748	Trendnet_cf:8c:04	Apple_92:6e:3d	EAPOL	133	Key
48.137310	Apple_92:6e:3d	Trendnet_cf:8c:04	EAPOL	157	Key
48.140357	Trendnet_cf:8c:04	Apple_92:6e:3d	EAPOL	157	Key
48.142945	Apple_92:6e:3d	Trendnet_cf:8c:04	EAPOL	133	Key

Figure 14:Eapol key,more in RFC5247.

5.3.4 Network Components Identified:

As in previous network capture we figure out what was the players in the capture.there was 12 conversation in 3A, and 18 in 3B,the pattern similar is the deauthentication against Apple-92:6e:3d,remarkable QoS amount between Vmware device and the Apple.

Cisco-Li_0c:7b:9c	Apple_92:6e:3d	64	12 219
Vmware_bc:b5:4b	Apple_92:6e:3d	148	16 120
Trendnet_cf:8c:04	Apple_92:6e:3d	271	8 274

Trendnet_cf:8c:04	Apple_92:6e:3d	266	7 837
Cisco-Li_0c:7b:9c	Apple_92:6e:3d	414	161 133
Vmware_bc:b5:4b	Apple_92:6e:3d	919	98 866

Figure 15:Players in 3A-3B Packet Capture.

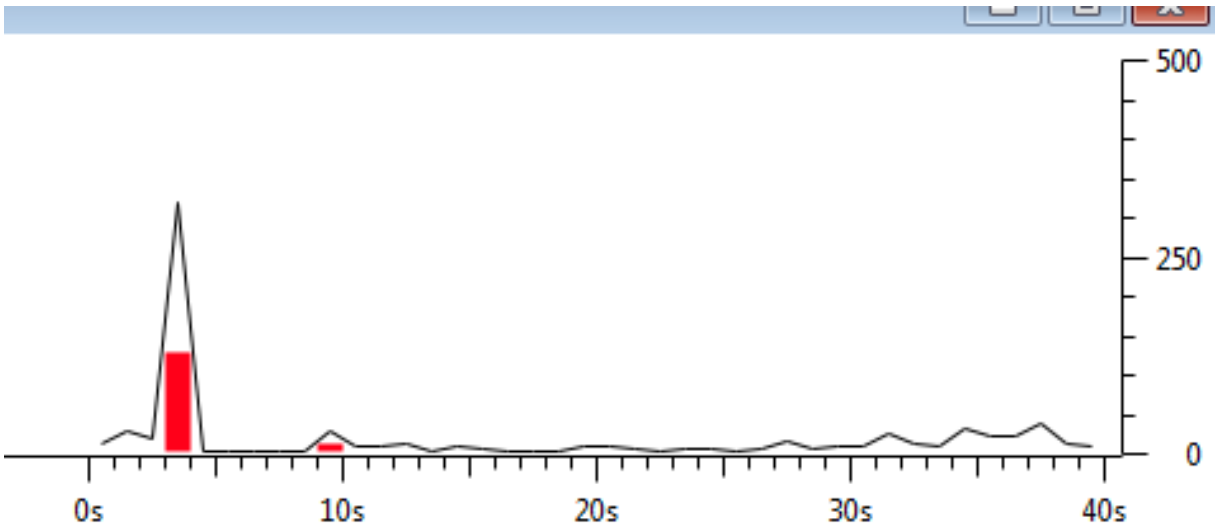
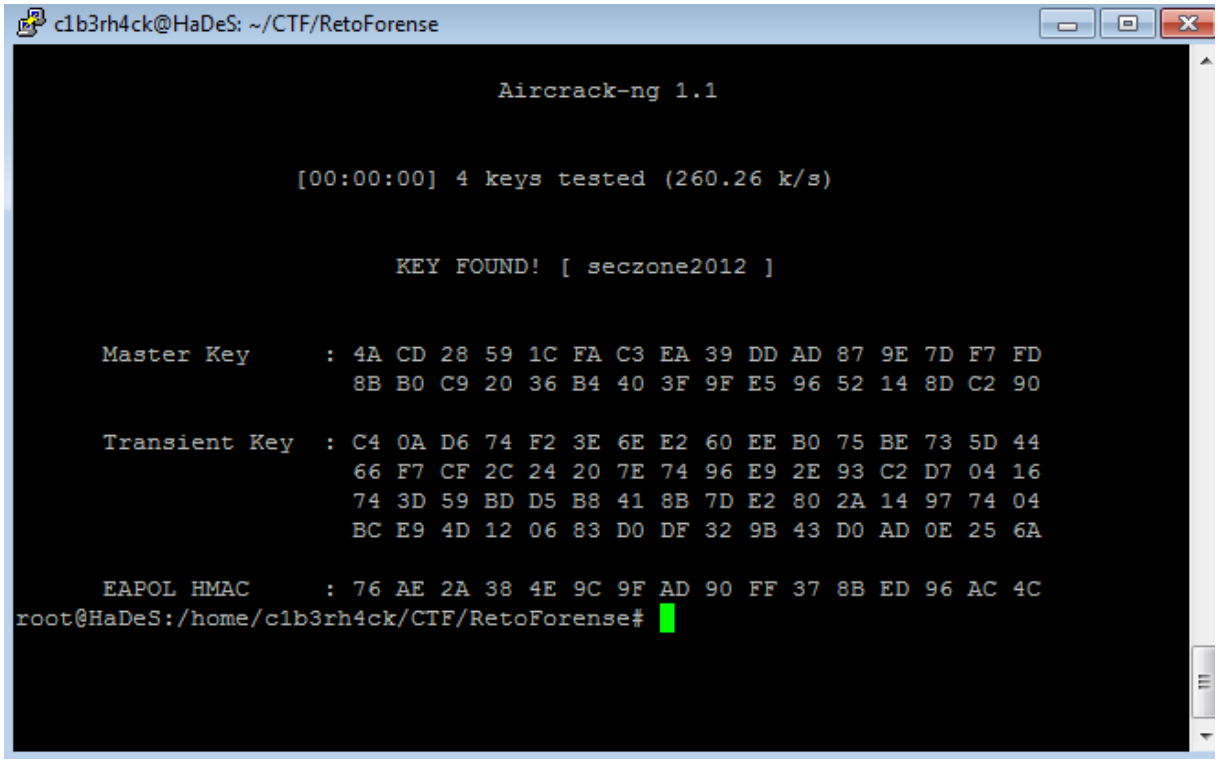


Figure 16:Graph shows up the network usage by Apple-92:6e:3d.



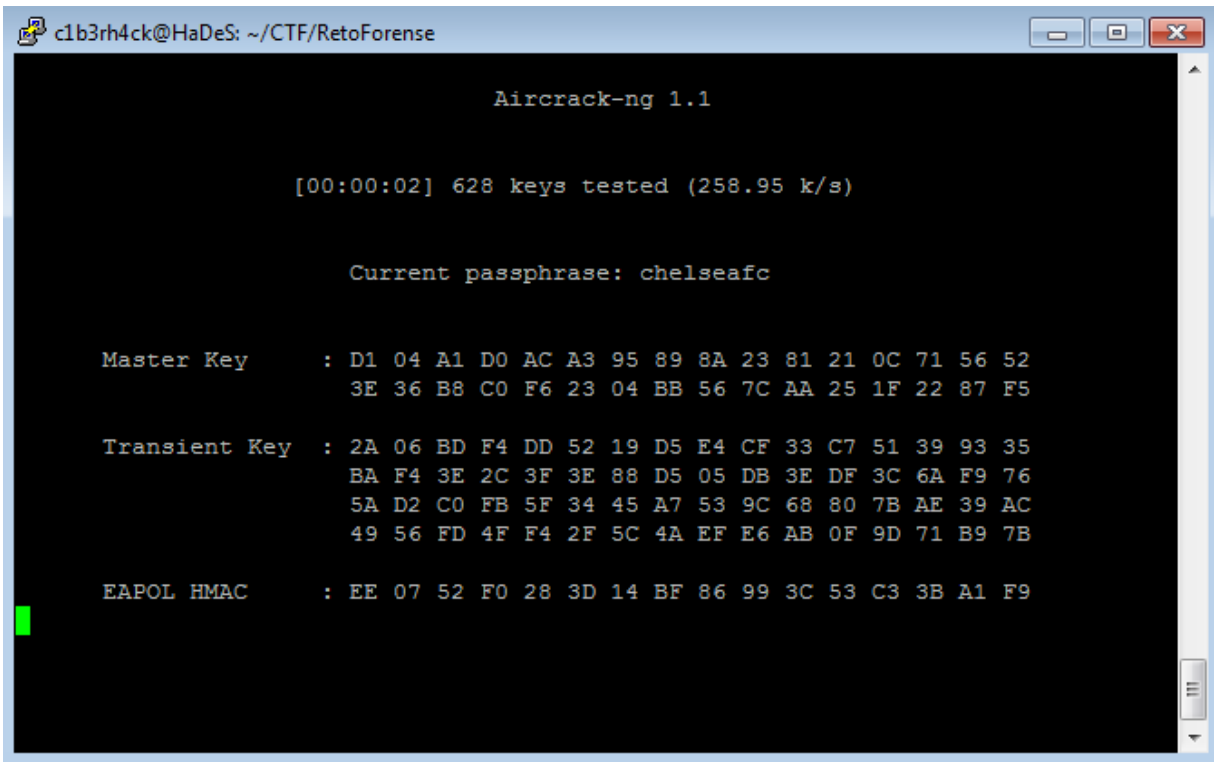


Figure 17:Aircrack bruteforce attack using the handshake in 3A,3B.

5.4 Network Capture CAPTURA4.:

Summary created by Wireshark (SVN Rev 51934 from /trunk-1.10)
File:
Name: C:/c1b3r/RetoForense/sPacketCapturesM - copia/CAPTURA4.cap
Length: 437594 bytes
Format: Wireshark/tcpdump/... - pcap
Encapsulation: Ethernet
Time:
First packet: **2013-07-25 01:18:20**
Last packet: **2013-07-25 01:19:28**
Elapsed: 00:01:07
Capture:
Unknown interface:
Dropped packets: unknown
Capture filter: unknown
Link type: IEEE 802.11 Wireless LAN
Packet size limit 65535 bytes
Statistics:
Packets: 404
Between first and last packet:67,927 sec
Avg. packets/sec: 5,948
Avg packet size: 1067,094 bytes
Bytes: 431106
Avg bytes/sec: 6346,569
Avg Mbit/sec: 0,051

5.4.1 Details CAPTURA4:

Reading the flow of packets I can see the conection between to ip addresses The network is reported to contain the activities of an individual operating with an IP address **190.157.162.25** and MAC **fe:ff:ff:ff:ff:ff** maybe a spoofed mac due to this is not on the list, of the vendor of the device's NIC. first few digits of the MAC address can be check here, is the same for **10.164.64.140**with MAC address **22:00:0a:40:8c**. The conversation is the access to a plattform that use Moodle a free software e-learning

platform with ip 190.157.162.25 and url http://curso.csiete.org/ this website use the amazon ec2 service although.In packet number 62 there is a user guest and password **guest** trying to log in

190.157.162.25 - Geo Information	
IP Address	190.157.162.25
Host	Dynamic-IP-19015716225.cable.net.co
Location	CO, Colombia
City	-, - -
Organization	Telmex Colombia S.A.
ISP	Telmex Colombia S.A.
AS Number	AS10620 Telmex Colombia S.A.
Latitude	4°00'00" North
Longitude	72°00'00" West
Distance	10138.68 km (6299.89 miles)

Figure 18: Whois information.

In packet number 130 we can see another user with session key Y4wOcoPOJY **guestpassword=12345** this login it seems successful because after that packet the user can see differents courses.

Stream Content

```
POST /enrol/index.php HTTP/1.1
Host: curso.csiete.org
Connection: keep-alive
Content-Length: 138
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Origin: http://curso.csiete.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/537.36 (KHTML
like Gecko) Chrome/28.0.1500.71 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: http://curso.csiete.org/enrol/index.php?id=2
Accept-Encoding: gzip,deflate,sdch
Accept-Language: es-ES,es;q=0.8
Cookie: MoodleSession=1ruoptqk9aom8nu82dc83eo9s7

id=2&instance=2&sesskey=Y4wOcoPOJY&_qf__enrol_guest_enrol_form=1&mform_isexpanded_id
estheader=1&guestpassword=12345&submitbutton=EnviarHTTP/1.1 303 See Other
Date: Thu, 25 Jul 2013 06:18:55 GMT
Server: Apache/2.2.24 (Amazon)
X-Powered-By: PHP/5.3.26
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
```

Figure 19: xform url encoded.

The other thing to notice here is the date **2013-07-25 01:18:20**, this packet capture is from is from july 25 and 5 of this network captures are from 2012 so A fact chronology can be a tremendous asset as you prepare a case for trial,in this case chronologies fail to live up to their full potential.A good chronology makes it easy for everyone on the trial team to share case knowledge.

6 References and Bibliography

1. ms-nlb-physerver
2. Ipv4 multicasm
3. SSDPV1
4. Embedded web server
5. Tshark Options
6. Probe Requests and Responses
7. A Standard for the Transmission of IP Datagrams over IEEE 802 Networks
8. Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition
9. Guide to Integrating Forensic Techniques into Incident Response
10. Extensible Authentication Protocol (EAP) Key Management Framework
11. Security Stackexchange – Wifi
12. Aireplay-Ng
13. 802.11 Network Forensic Analysis
14. Technical Report : Shedding Light on Data Correlation during Network Forensics Analysis
15. Understanding Wireless Attacks and Detection,Sans Institute
16. Case study: Network intrusion investigation e lessons in forensic preparation

7 Tools

- Virtualbox
- Wireshark
- Terminal Based Wireshark
- Coreutils
- Scapy
- PuTTY

8 Acknowledgement

I would like to express my deepest appreciation to all those(staff) who provided me the possibility to compete in this challenge,as a security enthusiast this is a great opportunity to search, read and learn something new in a field where I'm novice also because currently I'm a student and I don't have my own laptop :D, also thanks to every person who sincerely gave me their feedback, this exercises let me train and improve my network skills :).

BarcampSE v4.0 the great event that every year is growing up in Colombia.