Use any open-source software to capture the data of the application. For reference, from a pcap file, use any open-source software to extract each email (POP, IMAP, and SMTP protocols), all HTTP contents, and each VoIP call.

INTRODUCTION:

A .pcap file is a type of computer file that contains network traffic data captured by a network protocol analyzer tool such as Wireshark, tcpdump, or Tshark. The term "pcap" stands for "packet capture", and the file format is used to store network packets in a binary format.
When a network protocol analyzer tool captures network traffic, it captures packets in real time and stores them in a buffer. The captured packets can then be written to a .pcap file for further analysis, troubleshooting, or security auditing purposes.
In human language, a .pcap file is like a recording of all the data that flows through a network at a specific time. It can include information such as website requests and responses, emails, chat messages, video and audio calls, and any other data that is transmitted over the network. Analyzing a .pcap file can provide insight into network issues, security vulnerabilities, and performance problems.

There are three main email protocols used in email communication, which are as follows:

Simple Mail Transfer Protocol (SMTP): SMTP is a protocol used for sending emails between servers. When you compose and send an email, your email client communicates with your email server using SMTP to send the email to the recipient's email server.

Post Office Protocol (POP): POP is a protocol used by email clients to retrieve emails from an email server. When you open your email client, it connects to the email server using POP and downloads any new messages to your computer. The email messages are then deleted from the email server unless you have configured your email client to leave a copy of the messages on the server.

Internet Message Access Protocol (IMAP): IMAP is a protocol used by email clients to access and manage email messages stored on an email server. Unlike POP, IMAP allows you to keep a copy of the email messages on the email server, so you can access them from multiple devices. IMAP also supports features such as folder management, message search, and server-side filtering.

HTTP (Hypertext Transfer Protocol) is a protocol used for transmitting data over the internet. HTTP is the foundation of data communication for the World Wide Web. HTTP requests and responses are sent between web browsers and web servers, allowing users to access web pages and other online resources.
HTTP contents refer to the data transmitted in an HTTP request or response. The contents can include text, images, videos, audio files, and other types of data. HTTP requests typically include a URL (Uniform Resource Locator) that specifies the resource being requested, along with additional headers that provide information about the request.

HTTP responses include the requested resource, along with headers that provide information about the response, such as the content type, length, and caching information.

VoIP (Voice over Internet Protocol) is a technology used for transmitting voice and other multimedia data over the internet. VoIP enables users to make voice and video calls, send instant messages, and share files over IP networks. VoIP calls use a variety of protocols, including SIP (Session Initiation Protocol), H.323, and WebRTC.

During a VoIP call, the voice and video data is transmitted in packets over the network, much like other types of data. VoIP packets are typically small in size and must be transmitted with low latency to ensure real-time communication. VoIP also uses codecs to compress and decompress voice and video data, allowing it to be transmitted more efficiently over the network.

Scope of the project:

1)**Capturing network traffic:** Wireshark can capture network traffic on various types of networks, including Ethernet, Wi-Fi, and Bluetooth. It can capture data from both wired and wireless networks.

2**)Analyzing application protocols:** Wireshark can analyze a wide range of application protocols, such as HTTP, SMTP, FTP, POP, IMAP, and VoIP. It can extract specific data, such as email messages, from these protocols for further analysis.

3)**Identifying network issues:** Wireshark can be used to identify network issues such as slow performance, network congestion, and packet loss. It can also help identify security threats such as denial-of-service attacks, malware, and phishing.

4)**Troubleshooting network applications:** Wireshark can be used to troubleshoot issues with network applications, such as problems with file transfers or database queries.

System Description:

Target system description

For Wireshark to capture data from an application, it must be running on a system that is connected to the network being monitored. The target system for Wireshark can vary depending on the specific application being analyzed, but in general, the target system should meet the following requirements:

The system should be running an operating system that is supported by Wireshark. Wireshark is compatible with a wide range of operating systems, including Windows, Linux, and macOS.

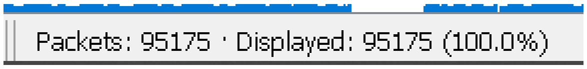
The system should have Wireshark installed and configured correctly. Wireshark can be downloaded for free from the Wireshark website, and installation instructions can be found in the

Wireshark User Guide.
The system should be connected to the network being monitored. This can be a wired or wireless network, depending on the type of traffic being analyzed.

The system should have the necessary permissions to capture network traffic. On Windows and macOS, this may require administrative privileges. On Linux, Wireshark may need to be run as root or with sudo privileges**.**

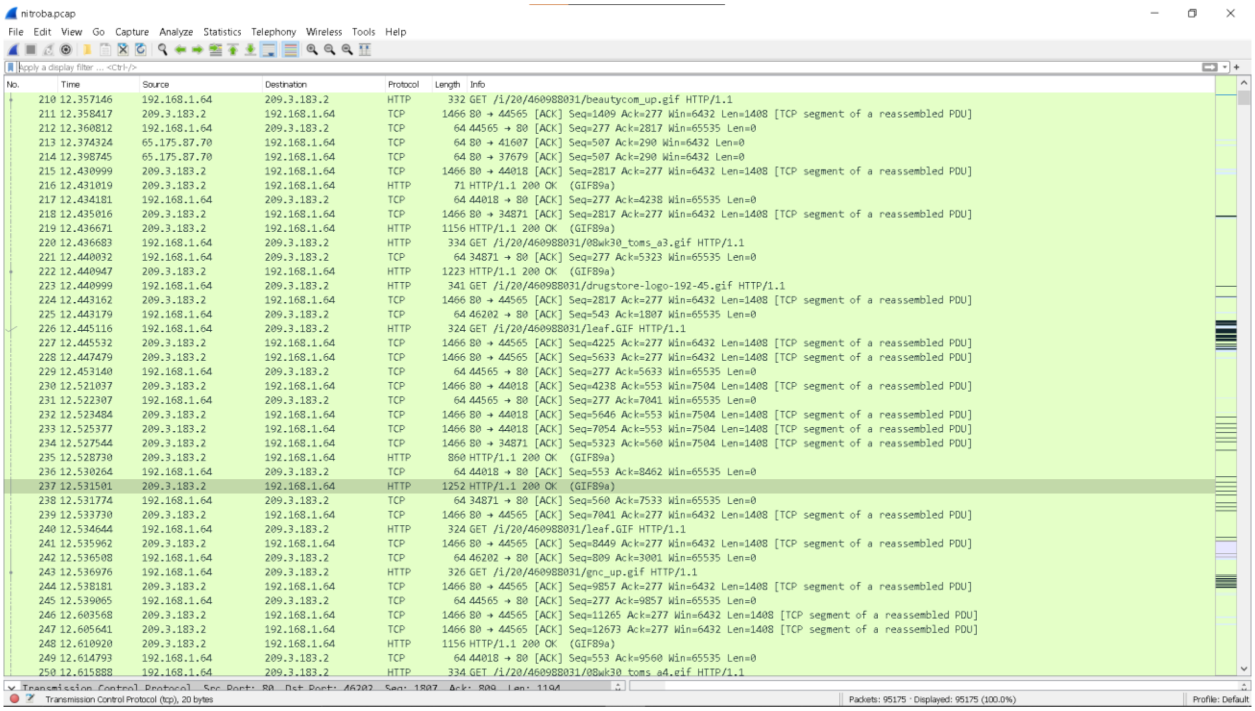
The dataset used in support of your project:

http://downloads.digitalcorpora.org/corpora/network-packet-dumps/2008-nitroba/nitroba.pcap.
(Or)
https://github.com/open-nsm/course/blob/master/pcaps/nitroba.pcap



```
Packets: 95175 · Displayed: 95175 (100.0%)
```

This file contains 95175 packets of different protocols.
Click on the PCAP file to open it in Wireshark. This will give you a first overview of the very long list of packets captured. The packets that are captured contains all the type of protocols and VoIP and HTTP



```
No.  Time       Source         Destination    Protocol Length Info
 210 12.357146  192.168.1.64   209.3.183.2    HTTP      332 GET /i/20/460988031/beautycom_up.gif HTTP/1.1
 211 12.358417  209.3.183.2    192.168.1.64   TCP      1466 80 → 44565 [ACK] Seq=1409 Ack=277 Win=6432 Len=1408 [TCP segment of a reassembled PDU]
 212 12.360812  192.168.1.64   209.3.183.2    TCP        64 44565 → 80 [ACK] Seq=277 Ack=2817 Win=65535 Len=0
 213 12.374324  65.175.87.70   192.168.1.64   TCP        64 80 → 41607 [ACK] Seq=507 Ack=290 Win=6432 Len=0
 214 12.398745  65.175.87.70   192.168.1.64   TCP        64 80 → 37679 [ACK] Seq=507 Ack=290 Win=6432 Len=0
 215 12.430999  209.3.183.2    192.168.1.64   TCP      1466 80 → 44018 [ACK] Seq=2817 Ack=277 Win=6432 Len=1408 [TCP segment of a reassembled PDU]
 216 12.431019  209.3.183.2    192.168.1.64   HTTP       71 HTTP/1.1 200 OK  (GIF89a)
 217 12.434181  192.168.1.64   209.3.183.2    TCP        64 44018 → 80 [ACK] Seq=277 Ack=4238 Win=65535 Len=0
 218 12.435016  209.3.183.2    192.168.1.64   TCP      1466 80 → 34871 [ACK] Seq=2817 Ack=277 Win=6432 Len=1408 [TCP segment of a reassembled PDU]
 219 12.436671  209.3.183.2    192.168.1.64   HTTP     1156 HTTP/1.1 200 OK  (GIF89a)
 220 12.436683  192.168.1.64   209.3.183.2    HTTP      334 GET /i/20/460988031/08wk30_toms_a3.gif HTTP/1.1
 221 12.440032  192.168.1.64   209.3.183.2    TCP        64 34871 → 80 [ACK] Seq=277 Ack=5323 Win=65535 Len=0
 222 12.440947  209.3.183.2    192.168.1.64   HTTP     1223 HTTP/1.1 200 OK  (GIF89a)
 223 12.440999  192.168.1.64   209.3.183.2    HTTP      341 GET /i/20/460988031/drugstore-logo-192-45.gif HTTP/1.1
 224 12.443162  209.3.183.2    192.168.1.64   TCP      1466 80 → 44565 [ACK] Seq=2817 Ack=277 Win=6432 Len=1408 [TCP segment of a reassembled PDU]
 225 12.443179  192.168.1.64   209.3.183.2    TCP        64 46202 → 80 [ACK] Seq=543 Ack=1807 Win=65535 Len=0
 226 12.445116  192.168.1.64   209.3.183.2    HTTP      324 GET /i/20/460988031/leaf.GIF HTTP/1.1
 227 12.445532  209.3.183.2    192.168.1.64   TCP      1466 80 → 44565 [ACK] Seq=4225 Ack=277 Win=6432 Len=1408 [TCP segment of a reassembled PDU]
 228 12.447479  209.3.183.2    192.168.1.64   TCP      1466 80 → 44565 [ACK] Seq=5633 Ack=277 Win=6432 Len=1408 [TCP segment of a reassembled PDU]
 229 12.453140  192.168.1.64   209.3.183.2    TCP        64 44565 → 80 [ACK] Seq=277 Ack=5633 Win=65535 Len=0
 230 12.521037  209.3.183.2    192.168.1.64   TCP      1466 80 → 44018 [ACK] Seq=4238 Ack=553 Win=7504 Len=1408 [TCP segment of a reassembled PDU]
 231 12.522307  192.168.1.64   209.3.183.2    TCP        64 44565 → 80 [ACK] Seq=277 Ack=7041 Win=65535 Len=0
 232 12.523484  209.3.183.2    192.168.1.64   TCP      1466 80 → 44018 [ACK] Seq=5646 Ack=553 Win=7504 Len=1408 [TCP segment of a reassembled PDU]
 233 12.525377  209.3.183.2    192.168.1.64   TCP      1466 80 → 44018 [ACK] Seq=7054 Ack=553 Win=7504 Len=1408 [TCP segment of a reassembled PDU]
 234 12.527544  209.3.183.2    192.168.1.64   TCP      1466 80 → 34871 [ACK] Seq=5323 Ack=560 Win=7504 Len=1408 [TCP segment of a reassembled PDU]
 235 12.528730  209.3.183.2    192.168.1.64   HTTP      860 HTTP/1.1 200 OK  (GIF89a)
 236 12.530264  192.168.1.64   209.3.183.2    TCP        64 44018 → 80 [ACK] Seq=553 Ack=8462 Win=65535 Len=0
 237 12.531501  209.3.183.2    192.168.1.64   HTTP     1252 HTTP/1.1 200 OK  (GIF89a)
 238 12.531774  192.168.1.64   209.3.183.2    TCP        64 34871 → 80 [ACK] Seq=560 Ack=7533 Win=65535 Len=0
 239 12.533730  209.3.183.2    192.168.1.64   TCP      1466 80 → 44565 [ACK] Seq=7041 Ack=277 Win=6432 Len=1408 [TCP segment of a reassembled PDU]
 240 12.534644  192.168.1.64   209.3.183.2    HTTP      324 GET /i/20/460988031/leaf.GIF HTTP/1.1
 241 12.535962  209.3.183.2    192.168.1.64   TCP      1466 80 → 44565 [ACK] Seq=8449 Ack=277 Win=6432 Len=1408 [TCP segment of a reassembled PDU]
 242 12.536508  192.168.1.64   209.3.183.2    TCP        64 46202 → 80 [ACK] Seq=809 Ack=3001 Win=65535 Len=0
 243 12.536976  192.168.1.64   209.3.183.2    HTTP      326 GET /i/20/460988031/gnc_up.gif HTTP/1.1
 244 12.538181  209.3.183.2    192.168.1.64   TCP      1466 80 → 44565 [ACK] Seq=9857 Ack=277 Win=6432 Len=1408 [TCP segment of a reassembled PDU]
 245 12.539065  192.168.1.64   209.3.183.2    TCP        64 44565 → 80 [ACK] Seq=277 Ack=9857 Win=65535 Len=0
 246 12.603568  209.3.183.2    192.168.1.64   TCP      1466 80 → 44565 [ACK] Seq=11265 Ack=277 Win=6432 Len=1408 [TCP segment of a reassembled PDU]
 247 12.605641  209.3.183.2    192.168.1.64   TCP      1466 80 → 44565 [ACK] Seq=12673 Ack=277 Win=6432 Len=1408 [TCP segment of a reassembled PDU]
 248 12.610920  209.3.183.2    192.168.1.64   HTTP     1156 HTTP/1.1 200 OK  (GIF89a)
 249 12.614793  192.168.1.64   209.3.183.2    TCP        64 44018 → 80 [ACK] Seq=553 Ack=9560 Win=65535 Len=0
 250 12.615888  192.168.1.64   209.3.183.2    HTTP      334 GET /i/20/460988031/08wk30_toms_a4.gif HTTP/1.1

Transmission Control Protocol, Src Port: 80, Dst Port: 46202, Seq: 1807, Ack: 809, Len: 1194
Transmission Control Protocol (tcp), 20 bytes      Packets: 95175 · Displayed: 95175 (100.0%)      Profile: Default
```

The first section lists the packets and frames in order by number, time, source IP, destination IP, protocol, and length. The second section provides information about the content of the packets and frames.

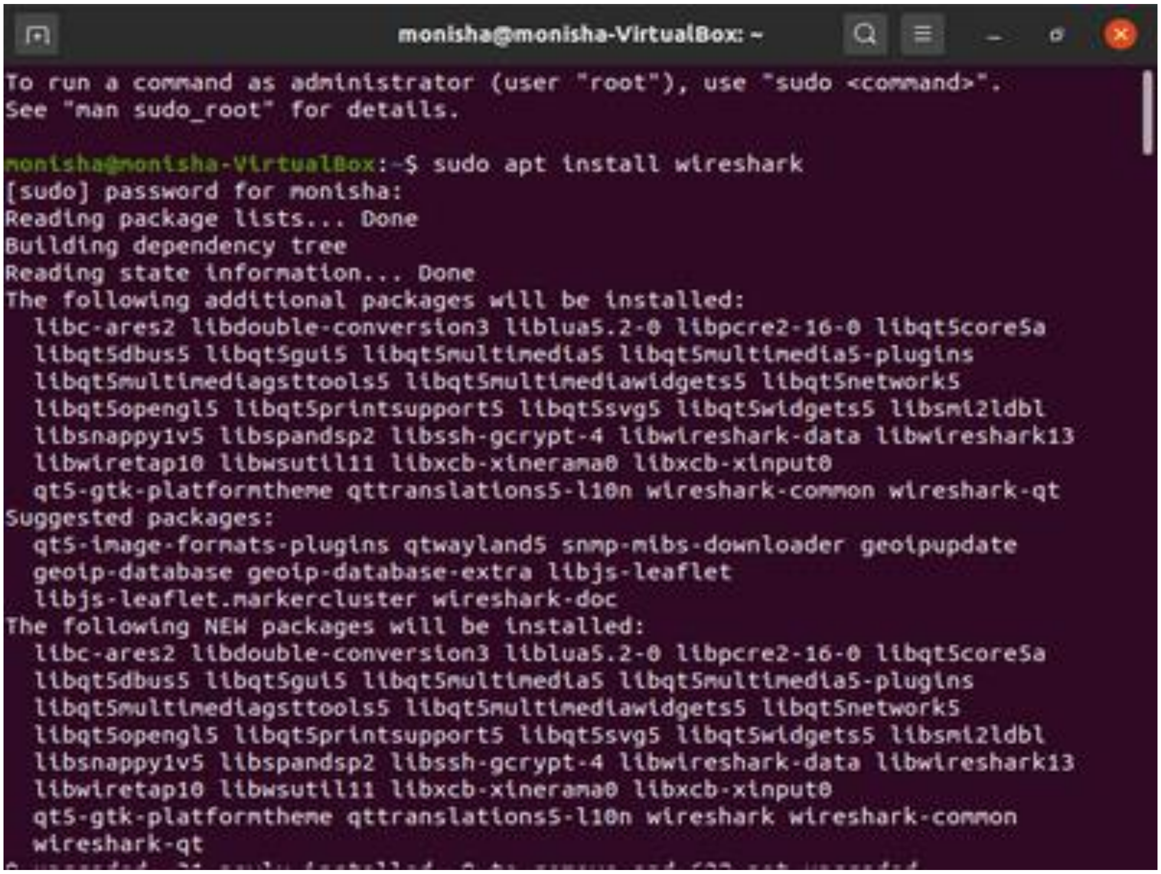
Once u click any packet the packet shows all the frames in order by source port, destination port, sequence number and etc…

Analysis Report:

To capture network traffic using Wireshark, we follow these steps:

1) Download and install Wireshark from the official website (https://www.wireshark.org/).
   (Or)

Install from Linux using the command **sudo apt install Wireshark (in figure 1)**

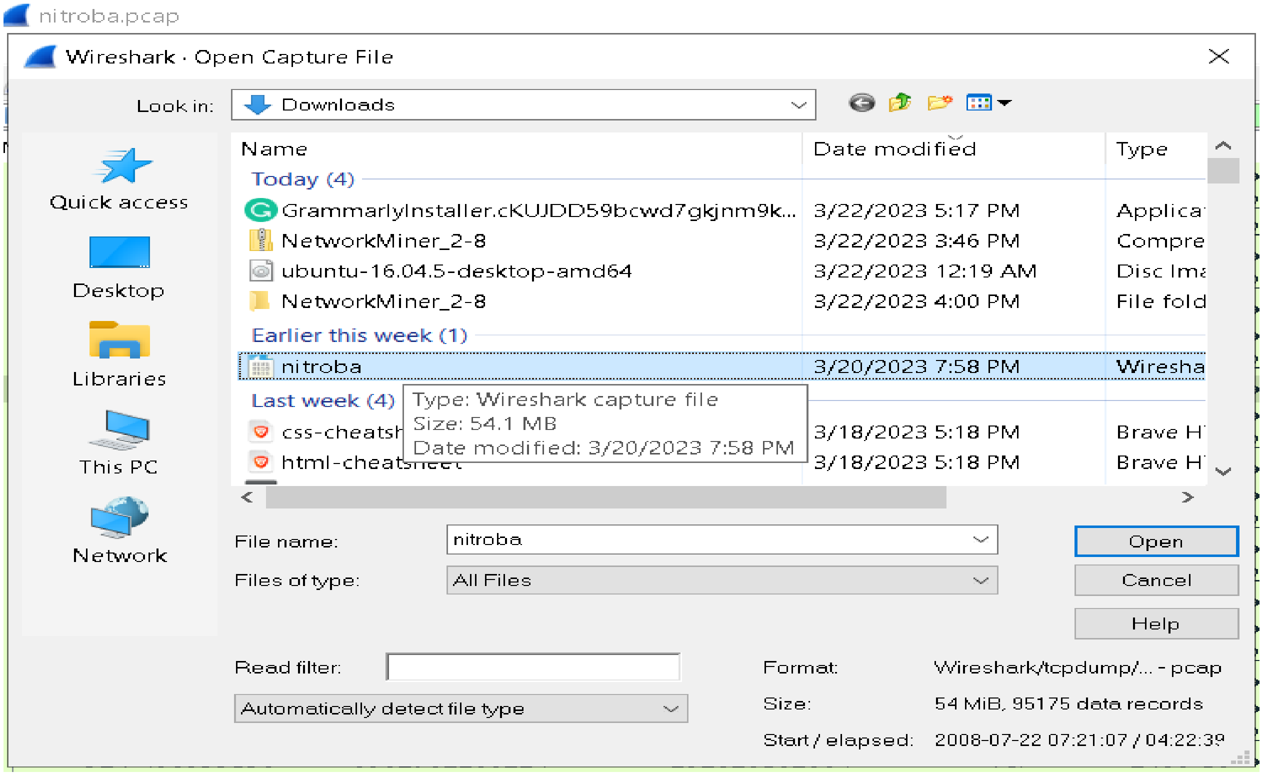


```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

monisha@monisha-VirtualBox:~$ sudo apt install wireshark
[sudo] password for monisha:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libc-ares2 libdouble-conversion3 liblua5.2-0 libpcre2-16-0 libqt5core5a
  libqt5dbus5 libqt5gui5 libqt5multimedia5 libqt5multimedia5-plugins
  libqt5multimediagsttools5 libqt5multimediawidgets5 libqt5network5
  libqt5opengl5 libqt5printsupport5 libqt5svg5 libqt5widgets5 libsmi2ldbl
  libsnappy1v5 libspandsp2 libssh-gcrypt-4 libwireshark-data libwireshark13
  libwiretap10 libwsutil11 libxcb-xinerama0 libxcb-xinput0
  qt5-gtk-platformtheme qttranslations5-l10n wireshark-common wireshark-qt
Suggested packages:
  qt5-image-formats-plugins qtwayland5 snmp-mibs-downloader geoipupdate
  geoip-database geoip-database-extra libjs-leaflet
  libjs-leaflet.markercluster wireshark-doc
The following NEW packages will be installed:
  libc-ares2 libdouble-conversion3 liblua5.2-0 libpcre2-16-0 libqt5core5a
  libqt5dbus5 libqt5gui5 libqt5multimedia5 libqt5multimedia5-plugins
  libqt5multimediagsttools5 libqt5multimediawidgets5 libqt5network5
  libqt5opengl5 libqt5printsupport5 libqt5svg5 libqt5widgets5 libsmi2ldbl
  libsnappy1v5 libspandsp2 libssh-gcrypt-4 libwireshark-data libwireshark13
  libwiretap10 libwsutil11 libxcb-xinerama0 libxcb-xinput0
  qt5-gtk-platformtheme qttranslations5-l10n wireshark wireshark-common
  wireshark-qt
```

Figure 1

2) Launch Wireshark and select the network interface you want to capture traffic on.(in fig 2)



nitroba.pcap

Wireshark · Open Capture File

Look in: Downloads

Name	Date modified	Type
Today (4)		
GrammarlyInstaller.cKUJDD59bcwd7gkjnm9k...	3/22/2023 5:17 PM	Applica
NetworkMiner_2-8	3/22/2023 3:46 PM	Compre
ubuntu-16.04.5-desktop-amd64	3/22/2023 12:19 AM	Disc Ima
NetworkMiner_2-8	3/22/2023 4:00 PM	File fold
Earlier this week (1)		
nitroba	3/20/2023 7:58 PM	Wiresha
Last week (4)		
css-cheatsh	3/18/2023 5:18 PM	Brave H
html-cheatsheet	3/18/2023 5:18 PM	Brave H

Type: Wireshark capture file
Size: 54.1 MB
Date modified: 3/20/2023 7:58 PM

File name: nitroba

Files of type: All Files

Read filter:

Automatically detect file type

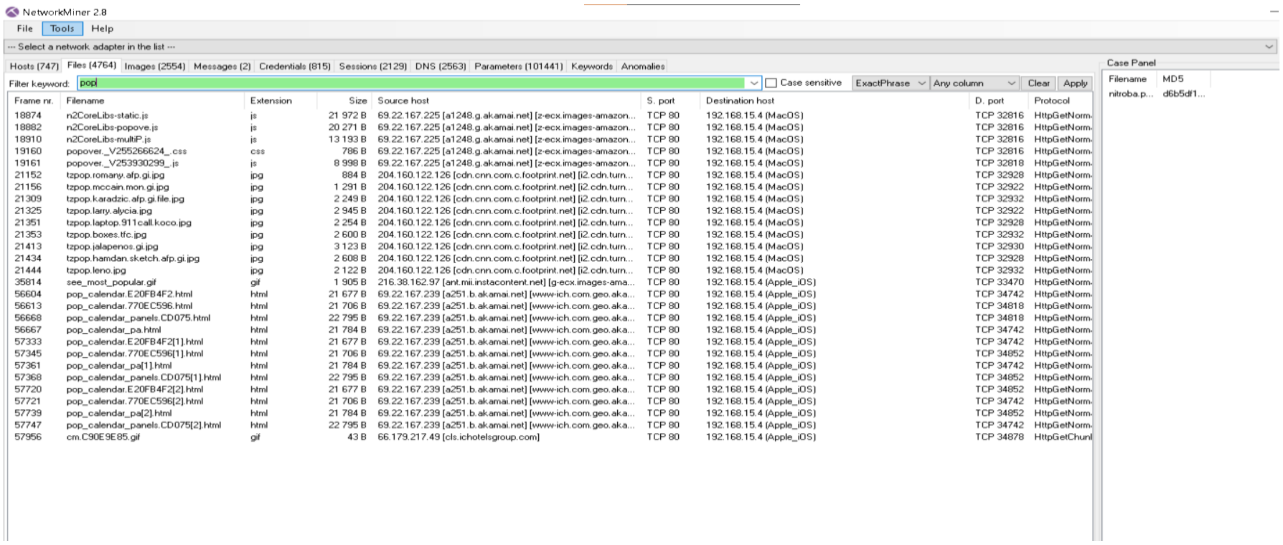
Format: Wireshark/tcpdump/... - pcap

Size: 54 MiB, 95175 data records

Start / elapsed: 2008-07-22 07:21:07 / 04:22:39

Figure 2

3) Click on the "Capture" button to start capturing traffic.
4) Use the filters to narrow down the traffic to the protocols you want to capture. For example, to capture email traffic, you can use filters for
   Pop – “pop”
   Smtp- “smtp”
   IMAP- “imap” (in fig 3)



NetworkMiner 2.8

--- Select a network adapter in the list ---

Hosts (747) | Files (4764) | Images (2554) | Messages (2) | Credentials (815) | Sessions (2129) | DNS (2563) | Parameters (101441) | Keywords | Anomalies

Filter keyword: pop   □ Case sensitive   ExactPhrase   Any column   Clear   Apply

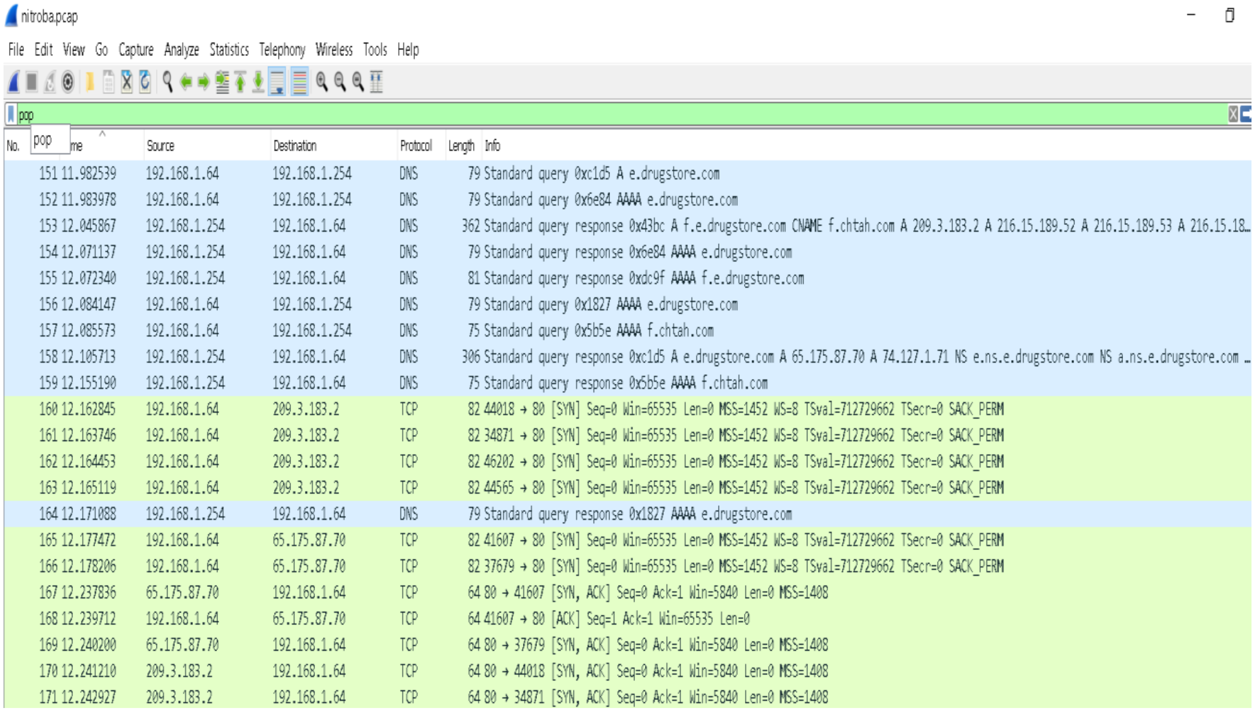
Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host	D. port	Protocol
18874	n2CoreLibs-static.js	js	21 972 B	69.22.167.225 [a1248.g.akamai.net] [z-ecx.images-amazon...	TCP 80	192.168.15.4 (MacOS)	TCP 32816	HttpGetNorm
18882	n2CoreLibs-popove.js	js	20 271 B	69.22.167.225 [a1248.g.akamai.net] [z-ecx.images-amazon...	TCP 80	192.168.15.4 (MacOS)	TCP 32816	HttpGetNorm
18910	n2CoreLibs-multiP.js	js	13 193 B	69.22.167.225 [a1248.g.akamai.net] [z-ecx.images-amazon...	TCP 80	192.168.15.4 (MacOS)	TCP 32816	HttpGetNorm
19160	popover._V255266624_.css	css	786 B	69.22.167.225 [a1248.g.akamai.net] [z-ecx.images-amazon...	TCP 80	192.168.15.4 (MacOS)	TCP 32816	HttpGetNorm
19161	popover._V253930299_.js	js	8 998 B	69.22.167.225 [a1248.g.akamai.net] [z-ecx.images-amazon...	TCP 80	192.168.15.4 (MacOS)	TCP 32818	HttpGetNorm
21152	tzpop.romany.afp.gi.jpg	jpg	884 B	204.160.122.126 [cdn.cnn.com.c.footprint.net] [i2.cdn.turn...	TCP 80	192.168.15.4 (MacOS)	TCP 32928	HttpGetNorm
21156	tzpop.mccain.mon.gi.jpg	jpg	1 291 B	204.160.122.126 [cdn.cnn.com.c.footprint.net] [i2.cdn.turn...	TCP 80	192.168.15.4 (MacOS)	TCP 32922	HttpGetNorm
21309	tzpop.karadzic.afp.gi.file.jpg	jpg	2 249 B	204.160.122.126 [cdn.cnn.com.c.footprint.net] [i2.cdn.turn...	TCP 80	192.168.15.4 (MacOS)	TCP 32932	HttpGetNorm
21325	tzpop.larry.alycia.jpg	jpg	2 945 B	204.160.122.126 [cdn.cnn.com.c.footprint.net] [i2.cdn.turn...	TCP 80	192.168.15.4 (MacOS)	TCP 32922	HttpGetNorm
21351	tzpop.laptop.911call.koco.jpg	jpg	2 254 B	204.160.122.126 [cdn.cnn.com.c.footprint.net] [i2.cdn.turn...	TCP 80	192.168.15.4 (MacOS)	TCP 32928	HttpGetNorm
21353	tzpop.boxes.tfc.jpg	jpg	2 600 B	204.160.122.126 [cdn.cnn.com.c.footprint.net] [i2.cdn.turn...	TCP 80	192.168.15.4 (MacOS)	TCP 32932	HttpGetNorm
21413	tzpop.jalapenos.gi.jpg	jpg	3 123 B	204.160.122.126 [cdn.cnn.com.c.footprint.net] [i2.cdn.turn...	TCP 80	192.168.15.4 (MacOS)	TCP 32930	HttpGetNorm
21434	tzpop.hamdan.sketch.afp.gi.jpg	jpg	2 608 B	204.160.122.126 [cdn.cnn.com.c.footprint.net] [i2.cdn.turn...	TCP 80	192.168.15.4 (MacOS)	TCP 32928	HttpGetNorm
21444	tzpop.leno.jpg	jpg	2 122 B	204.160.122.126 [cdn.cnn.com.c.footprint.net] [i2.cdn.turn...	TCP 80	192.168.15.4 (MacOS)	TCP 32932	HttpGetNorm
35814	see_most_popular.gif	gif	1 905 B	216.38.162.97 [ant.mii.instacontent.net] [g-ecx.images-ama...	TCP 80	192.168.15.4 (Apple_iOS)	TCP 33470	HttpGetNorm
56604	pop_calendar.E20FB4F2.html	html	21 677 B	69.22.167.239 [a251.b.akamai.net] [www-ich.com.geo.aka...	TCP 80	192.168.15.4 (Apple_iOS)	TCP 34742	HttpGetNorm
56613	pop_calendar.770EC596.html	html	21 706 B	69.22.167.239 [a251.b.akamai.net] [www-ich.com.geo.aka...	TCP 80	192.168.15.4 (Apple_iOS)	TCP 34818	HttpGetNorm
56668	pop_calendar_panels.CD075.html	html	22 795 B	69.22.167.239 [a251.b.akamai.net] [www-ich.com.geo.aka...	TCP 80	192.168.15.4 (Apple_iOS)	TCP 34818	HttpGetNorm
56667	pop_calendar_pa.html	html	21 784 B	69.22.167.239 [a251.b.akamai.net] [www-ich.com.geo.aka...	TCP 80	192.168.15.4 (Apple_iOS)	TCP 34742	HttpGetNorm
57333	pop_calendar.E20FB4F2[1].html	html	21 677 B	69.22.167.239 [a251.b.akamai.net] [www-ich.com.geo.aka...	TCP 80	192.168.15.4 (Apple_iOS)	TCP 34742	HttpGetNorm
57345	pop_calendar.770EC596[1].html	html	21 706 B	69.22.167.239 [a251.b.akamai.net] [www-ich.com.geo.aka...	TCP 80	192.168.15.4 (Apple_iOS)	TCP 34852	HttpGetNorm
57361	pop_calendar_pa[1].html	html	21 784 B	69.22.167.239 [a251.b.akamai.net] [www-ich.com.geo.aka...	TCP 80	192.168.15.4 (Apple_iOS)	TCP 34742	HttpGetNorm
57368	pop_calendar_panels.CD075[1].html	html	22 795 B	69.22.167.239 [a251.b.akamai.net] [www-ich.com.geo.aka...	TCP 80	192.168.15.4 (Apple_iOS)	TCP 34852	HttpGetNorm
57720	pop_calendar.E20FB4F2[2].html	html	21 677 B	69.22.167.239 [a251.b.akamai.net] [www-ich.com.geo.aka...	TCP 80	192.168.15.4 (Apple_iOS)	TCP 34852	HttpGetNorm
57721	pop_calendar.770EC596[2].html	html	21 706 B	69.22.167.239 [a251.b.akamai.net] [www-ich.com.geo.aka...	TCP 80	192.168.15.4 (Apple_iOS)	TCP 34742	HttpGetNorm
57739	pop_calendar_pa[2].html	html	21 784 B	69.22.167.239 [a251.b.akamai.net] [www-ich.com.geo.aka...	TCP 80	192.168.15.4 (Apple_iOS)	TCP 34852	HttpGetNorm
57747	pop_calendar_panels.CD075[2].html	html	22 795 B	69.22.167.239 [a251.b.akamai.net] [www-ich.com.geo.aka...	TCP 80	192.168.15.4 (Apple_iOS)	TCP 34742	HttpGetNorm
57956	cm.C90E9E85.gif	gif	43 B	66.179.217.49 [cls.ichotelsgroup.com]	TCP 80	192.168.15.4 (Apple_iOS)	TCP 34878	HttpGetChunl

Case Panel

Filename	MD5
nitroba.p...	d6b5df1...

Figure 3

This is done in **NETWORK MINER (in fig 4)**


nitroba.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

pop

No.	me	Source	Destination	Protocol	Length	Info
151	11.982539	192.168.1.64	192.168.1.254	DNS	79	Standard query 0xc1d5 A e.drugstore.com
152	11.983978	192.168.1.64	192.168.1.254	DNS	79	Standard query 0x6e84 AAAA e.drugstore.com
153	12.045867	192.168.1.254	192.168.1.64	DNS	362	Standard query response 0x43bc A f.e.drugstore.com CNAME f.chtah.com A 209.3.183.2 A 216.15.189.52 A 216.15.189.53 A 216.15.18…
154	12.071137	192.168.1.254	192.168.1.64	DNS	79	Standard query response 0x6e84 AAAA e.drugstore.com
155	12.072340	192.168.1.254	192.168.1.64	DNS	81	Standard query response 0xdc9f AAAA f.e.drugstore.com
156	12.084147	192.168.1.64	192.168.1.254	DNS	79	Standard query 0x1827 AAAA e.drugstore.com
157	12.085573	192.168.1.64	192.168.1.254	DNS	75	Standard query 0x5b5e AAAA f.chtah.com
158	12.105713	192.168.1.254	192.168.1.64	DNS	306	Standard query response 0xc1d5 A e.drugstore.com A 65.175.87.70 A 74.127.1.71 NS e.ns.e.drugstore.com NS a.ns.e.drugstore.com …
159	12.155190	192.168.1.254	192.168.1.64	DNS	75	Standard query response 0x5b5e AAAA f.chtah.com
160	12.162845	192.168.1.64	209.3.183.2	TCP	82	44018 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1452 WS=8 TSval=712729662 TSecr=0 SACK_PERM
161	12.163746	192.168.1.64	209.3.183.2	TCP	82	34871 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1452 WS=8 TSval=712729662 TSecr=0 SACK_PERM
162	12.164453	192.168.1.64	209.3.183.2	TCP	82	46202 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1452 WS=8 TSval=712729662 TSecr=0 SACK_PERM
163	12.165119	192.168.1.64	209.3.183.2	TCP	82	44565 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1452 WS=8 TSval=712729662 TSecr=0 SACK_PERM
164	12.171088	192.168.1.254	192.168.1.64	DNS	79	Standard query response 0x1827 AAAA e.drugstore.com
165	12.177472	192.168.1.64	65.175.87.70	TCP	82	41607 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1452 WS=8 TSval=712729662 TSecr=0 SACK_PERM
166	12.178206	192.168.1.64	65.175.87.70	TCP	82	37679 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1452 WS=8 TSval=712729662 TSecr=0 SACK_PERM
167	12.237836	65.175.87.70	192.168.1.64	TCP	64	80 → 41607 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1408
168	12.239712	192.168.1.64	65.175.87.70	TCP	64	41607 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
169	12.240200	65.175.87.70	192.168.1.64	TCP	64	80 → 37679 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1408
170	12.241210	209.3.183.2	192.168.1.64	TCP	64	80 → 44018 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1408
171	12.242927	209.3.183.2	192.168.1.64	TCP	64	80 → 34871 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1408

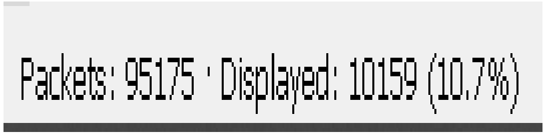
Figure 4

We will change the filter from pop to “smtp” or “imap” so that we can get the smtp and imap files.
(The data file doesn’t contain any smtp or imap packets)

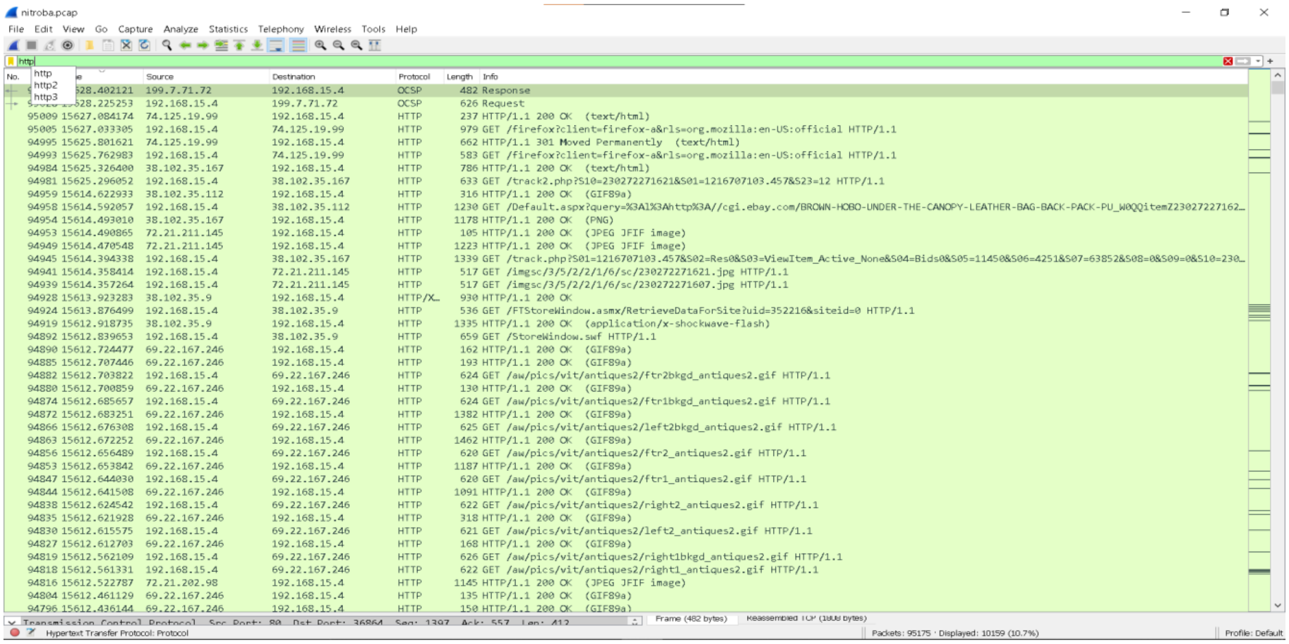
5) Once the filtered traffic is displayed, select the desired packet and right-click on it to select "Follow > TCP Stream" (for SMTP) or "Follow > TCP Stream > Assemble" (for POP/IMAP). (will be shown for http content)

For HTTP content

1) To filter HTTP traffic, enter "http" in the filter box at the top of the Wireshark window. This will display only HTTP traffic in the capture. (in figure 5)



Packets: 95175 · Displayed: 10159 (10.7%)


nitroba.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
http
http2
http3

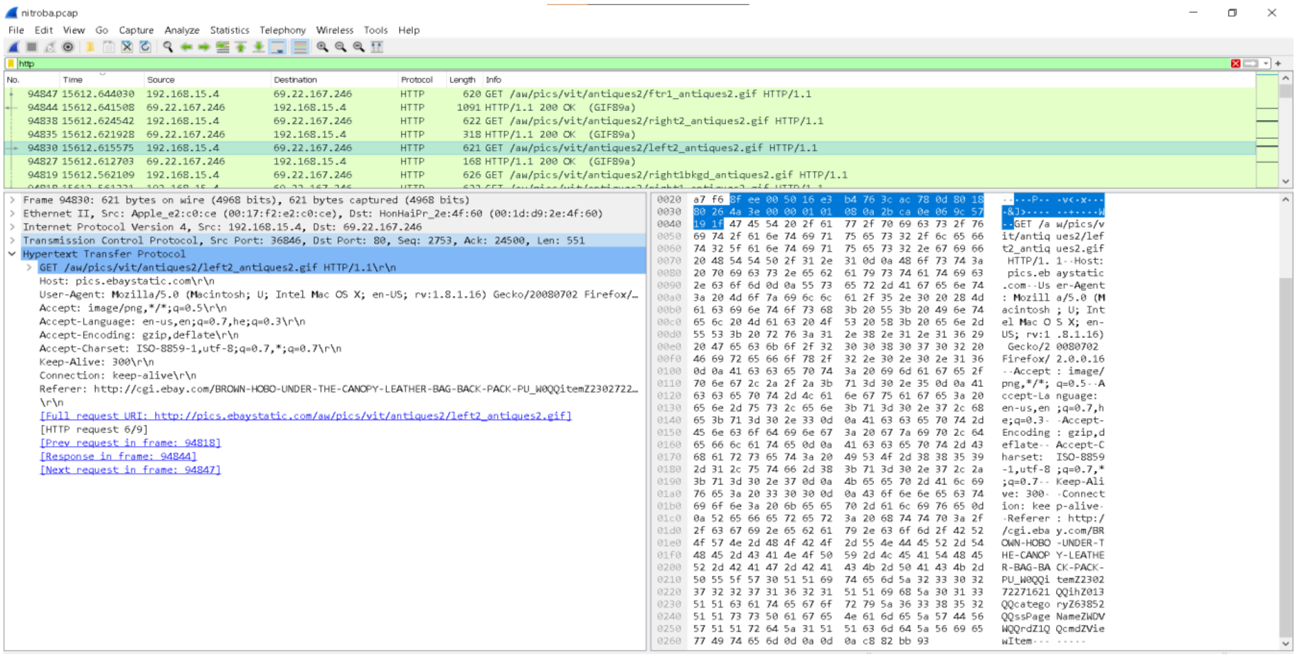
```
No.   Time              Source          Destination     Protocol Length Info
9     528.402121        199.7.71.72     192.168.15.4    OCSP      482 Response
      528.225253        192.168.15.4    199.7.71.72     OCSP      626 Request
95009 15627.084174 74.125.19.99    192.168.15.4    HTTP      237 HTTP/1.1 200 OK  (text/html)
95005 15627.033305 192.168.15.4    74.125.19.99    HTTP      979 GET /firefox?client=firefox-a&rls=org.mozilla:en-US:official HTTP/1.1
94995 15625.801621 74.125.19.99    192.168.15.4    HTTP      662 HTTP/1.1 301 Moved Permanently  (text/html)
94993 15625.762983 192.168.15.4    74.125.19.99    HTTP      583 GET /firefox?client=firefox-a&rls=org.mozilla:en-US:official HTTP/1.1
94984 15625.326400 38.102.35.167   192.168.15.4    HTTP      786 HTTP/1.1 200 OK  (text/html)
94981 15625.296052 192.168.15.4    38.102.35.167   HTTP      633 GET /track2.php?S10=230272271621&S01=1216707103.457&S23=12 HTTP/1.1
94959 15614.622933 38.102.35.112   192.168.15.4    HTTP      316 HTTP/1.1 200 OK  (GIF89a)
94958 15614.592057 192.168.15.4    38.102.35.112   HTTP     1230 GET /Default.aspx?query=%3A1%3Ahttp%3A//cgi.ebay.com/BROWN-HOBO-UNDER-THE-CANOPY-LEATHER-BAG-BACK-PACK-PU_W0QQitemZ23027227162…
94954 15614.493010 38.102.35.167   192.168.15.4    HTTP     1178 HTTP/1.1 200 OK  (PNG)
94953 15614.490865 72.21.211.145   192.168.15.4    HTTP      105 HTTP/1.1 200 OK  (JPEG JFIF image)
94949 15614.470548 72.21.211.145   192.168.15.4    HTTP     1223 HTTP/1.1 200 OK  (JPEG JFIF image)
94945 15614.394338 192.168.15.4    38.102.35.167   HTTP     1339 GET /track.php?S01=1216707103.457&S02=Res0&S03=ViewItem_Active_None&S04=Bids0&S05=11450&S06=4251&S07=63852&S08=0&S09=0&S10=230…
94941 15614.358414 192.168.15.4    72.21.211.145   HTTP      517 GET /imgsc/3/5/2/2/1/6/sc/230272271621.jpg HTTP/1.1
94939 15614.357264 192.168.15.4    72.21.211.145   HTTP      517 GET /imgsc/3/5/2/2/1/6/sc/230272271607.jpg HTTP/1.1
94928 15613.923283 38.102.35.9     192.168.15.4    HTTP/X…   930 HTTP/1.1 200 OK
94924 15613.876499 192.168.15.4    38.102.35.9     HTTP      536 GET /FTStoreWindow.asmx/RetrieveDataForSite?uid=352216&siteid=0 HTTP/1.1
94919 15612.918735 38.102.35.9     192.168.15.4    HTTP     1335 HTTP/1.1 200 OK  (application/x-shockwave-flash)
94892 15612.839653 192.168.15.4    38.102.35.9     HTTP      659 GET /StoreWindow.swf HTTP/1.1
94890 15612.724477 69.22.167.246   192.168.15.4    HTTP      162 HTTP/1.1 200 OK  (GIF89a)
94885 15612.707446 69.22.167.246   192.168.15.4    HTTP      193 HTTP/1.1 200 OK  (GIF89a)
94882 15612.703822 192.168.15.4    69.22.167.246   HTTP      624 GET /aw/pics/vit/antiques2/ftr2bkgd_antiques2.gif HTTP/1.1
94880 15612.700859 69.22.167.246   192.168.15.4    HTTP      130 HTTP/1.1 200 OK  (GIF89a)
94874 15612.685657 192.168.15.4    69.22.167.246   HTTP      624 GET /aw/pics/vit/antiques2/ftr1bkgd_antiques2.gif HTTP/1.1
94872 15612.683251 69.22.167.246   192.168.15.4    HTTP     1382 HTTP/1.1 200 OK  (GIF89a)
94866 15612.676308 192.168.15.4    69.22.167.246   HTTP      625 GET /aw/pics/vit/antiques2/left2bkgd_antiques2.gif HTTP/1.1
94863 15612.672252 69.22.167.246   192.168.15.4    HTTP     1462 HTTP/1.1 200 OK  (GIF89a)
94856 15612.656489 192.168.15.4    69.22.167.246   HTTP      620 GET /aw/pics/vit/antiques2/ftr2_antiques2.gif HTTP/1.1
94853 15612.653842 69.22.167.246   192.168.15.4    HTTP     1187 HTTP/1.1 200 OK  (GIF89a)
94847 15612.644030 192.168.15.4    69.22.167.246   HTTP      620 GET /aw/pics/vit/antiques2/ftr1_antiques2.gif HTTP/1.1
94844 15612.641508 69.22.167.246   192.168.15.4    HTTP     1091 HTTP/1.1 200 OK  (GIF89a)
94838 15612.624542 192.168.15.4    69.22.167.246   HTTP      622 GET /aw/pics/vit/antiques2/right2_antiques2.gif HTTP/1.1
94835 15612.621928 69.22.167.246   192.168.15.4    HTTP      318 HTTP/1.1 200 OK  (GIF89a)
94830 15612.615575 192.168.15.4    69.22.167.246   HTTP      621 GET /aw/pics/vit/antiques2/left2_antiques2.gif HTTP/1.1
94827 15612.612703 69.22.167.246   192.168.15.4    HTTP      168 HTTP/1.1 200 OK  (GIF89a)
94819 15612.562109 192.168.15.4    69.22.167.246   HTTP      626 GET /aw/pics/vit/antiques2/right1bkgd_antiques2.gif HTTP/1.1
94818 15612.561331 192.168.15.4    69.22.167.246   HTTP      622 GET /aw/pics/vit/antiques2/right1_antiques2.gif HTTP/1.1
94816 15612.522787 72.21.202.98    192.168.15.4    HTTP     1145 HTTP/1.1 200 OK  (JPEG JFIF image)
94804 15612.461129 69.22.167.246   192.168.15.4    HTTP      135 HTTP/1.1 200 OK  (GIF89a)
94796 15612.436144 69.22.167.246   192.168.15.4    HTTP      150 HTTP/1.1 200 OK  (GIF89a)

Transmission Control Protocol, Src Port: 80, Dst Port: 36864, Seq: 1397, Ack: 557, Len: 412
Frame (482 bytes)   Reassembled TCP (1808 bytes)
Hypertext Transfer Protocol: Protocol        Packets: 95175 · Displayed: 10159 (10.7%)        Profile: Default
```

Figure 5

The http filter has filtered all the http content from all the udp and tcp contents

2) To view the contents of an HTTP packet, select the packet in the packet list pane and then expand the "Hypertext Transfer Protocol" section in the packet details pane. You can see the full contents of the HTTP request and response.(in figure 6)


nitroba.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time              Source          Destination     Protocol Length Info
94847 15612.644030 192.168.15.4    69.22.167.246   HTTP      620 GET /aw/pics/vit/antiques2/ftr1_antiques2.gif HTTP/1.1
94844 15612.641508 69.22.167.246   192.168.15.4    HTTP     1091 HTTP/1.1 200 OK  (GIF89a)
94838 15612.624542 192.168.15.4    69.22.167.246   HTTP      622 GET /aw/pics/vit/antiques2/right2_antiques2.gif HTTP/1.1
94835 15612.621928 69.22.167.246   192.168.15.4    HTTP      318 HTTP/1.1 200 OK  (GIF89a)
94830 15612.615575 192.168.15.4    69.22.167.246   HTTP      621 GET /aw/pics/vit/antiques2/left2_antiques2.gif HTTP/1.1
94827 15612.612703 69.22.167.246   192.168.15.4    HTTP      168 HTTP/1.1 200 OK  (GIF89a)
94819 15612.562109 192.168.15.4    69.22.167.246   HTTP      626 GET /aw/pics/vit/antiques2/right1bkgd_antiques2.gif HTTP/1.1
94818 15612.561331 192.168.15.4    69.22.167.246   HTTP      622 GET /aw/pics/vit/antiques2/right1_antiques2.gif HTTP/1.1
```

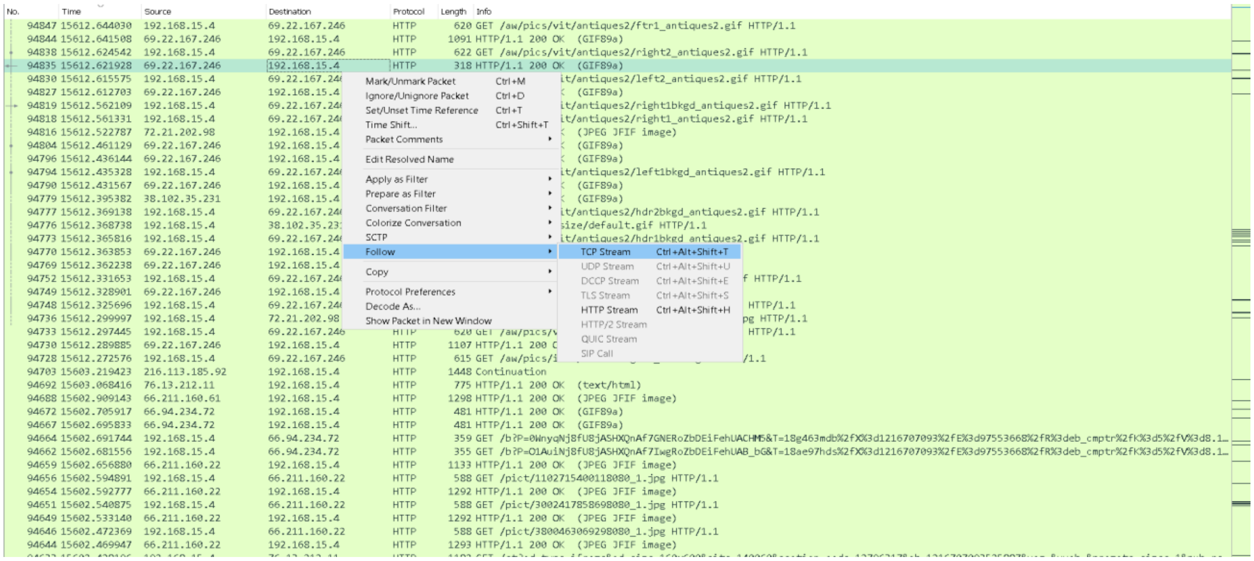
```
> Frame 94830: 621 bytes on wire (4968 bits), 621 bytes captured (4968 bits)
> Ethernet II, Src: Apple_e2:c0:ce (00:17:f2:e2:c0:ce), Dst: HonHaiPr_2e:4f:60 (00:1d:d9:2e:4f:60)
> Internet Protocol Version 4, Src: 192.168.15.4, Dst: 69.22.167.246
> Transmission Control Protocol, Src Port: 36846, Dst Port: 80, Seq: 2753, Ack: 24500, Len: 551
v Hypertext Transfer Protocol
  > GET /aw/pics/vit/antiques2/left2_antiques2.gif HTTP/1.1\r\n
    Host: pics.ebaystatic.com\r\n
    User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X; en-US; rv:1.8.1.16) Gecko/20080702 Firefox/…
    Accept: image/png,*/*;q=0.5\r\n
    Accept-Language: en-us,en;q=0.7,he;q=0.3\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    Referer: http://cgi.ebay.com/BROWN-HOBO-UNDER-THE-CANOPY-LEATHER-BAG-BACK-PACK-PU_W0QQitemZ2302722…
    \r\n
    [Full request URI: http://pics.ebaystatic.com/aw/pics/vit/antiques2/left2_antiques2.gif]
    [HTTP request 6/9]
    [Prev request in frame: 94818]
    [Response in frame: 94844]
    [Next request in frame: 94847]
```

```
0020  a7 f6 8f ee 00 50 16 e3  b4 76 3c ac 78 0d 80 18   ·····P·· ·v<·x···
0030  80 26 4a 3e 00 00 01 01  08 0a 2b ca 0e 06 9c 57   ·&J>···· ··+····W
0040  19 1f 47 45 54 20 2f 61  77 2f 70 69 63 73 2f 76   ··GET /a w/pics/v
0050  69 74 2f 61 6e 74 69 71  75 65 73 32 2f 6c 65 66   it/antiq ues2/lef
0060  74 32 5f 61 6e 74 69 71  75 65 73 32 2e 67 69 66   t2_antiq ues2.gif
0070  20 48 54 54 50 2f 31 2e  31 0d 0a 48 6f 73 74 3a    HTTP/1. 1··Host:
0080  20 70 69 63 73 2e 65 62  61 79 73 74 61 74 69 63    pics.eb aystatic
0090  2e 63 6f 6d 0d 0a 55 73  65 72 2d 41 67 65 6e 74   .com··Us er-Agent
00a0  3a 20 4d 6f 7a 69 6c 6c  61 2f 35 2e 30 20 28 4d   : Mozill a/5.0 (M
00b0  61 63 69 6e 74 6f 73 68  3b 20 55 3b 20 49 6e 74   acintosh ; U; Int
00c0  65 6c 20 4d 61 63 20 4f  53 20 58 3b 20 65 6e 2d   el Mac O S X; en-
00d0  55 53 3b 20 72 76 3a 31  2e 38 2e 31 2e 31 36 29   US; rv:1 .8.1.16)
00e0  20 47 65 63 6b 6f 2f 32  30 30 38 30 37 30 32 20    Gecko/2 0080702 
00f0  46 69 72 65 66 6f 78 2f  32 2e 30 2e 30 2e 31 36   Firefox/ 2.0.0.16
0100  0d 0a 41 63 63 65 70 74  3a 20 69 6d 61 67 65 2f   ··Accept : image/
0110  70 6e 67 2c 2a 2f 2a 3b  71 3d 30 2e 35 0d 0a 41   png,*/*; q=0.5··A
0120  63 63 65 70 74 2d 4c 61  6e 67 75 61 67 65 3a 20   ccept-La nguage: 
0130  65 6e 2d 75 73 2c 65 6e  3b 71 3d 30 2e 37 2c 68   en-us,en ;q=0.7,h
0140  65 3b 71 3d 30 2e 33 0d  0a 41 63 63 65 70 74 2d   e;q=0.3· ·Accept-
0150  45 6e 63 6f 64 69 6e 67  3a 20 67 7a 69 70 2c 64   Encoding : gzip,d
0160  65 66 6c 61 74 65 0d 0a  41 63 63 65 70 74 2d 43   eflate·· Accept-C
0170  68 61 72 73 65 74 3a 20  49 53 4f 2d 38 38 35 39   harset:  ISO-8859
0180  2d 31 2c 75 74 66 2d 38  3b 71 3d 30 2e 37 2c 2a   -1,utf-8 ;q=0.7,*
0190  3b 71 3d 30 2e 37 0d 0a  4b 65 65 70 2d 41 6c 69   ;q=0.7·· Keep-Ali
01a0  76 65 3a 20 33 30 30 0d  0a 43 6f 6e 6e 65 63 74   ve: 300· ·Connect
01b0  69 6f 6e 3a 20 6b 65 65  70 2d 61 6c 69 76 65 0d   ion: kee p-alive·
01c0  0a 52 65 66 65 72 65 72  3a 20 68 74 74 70 3a 2f   ·Referer : http:/
01d0  2f 63 67 69 2e 65 62 61  79 2e 63 6f 6d 2f 42 52   /cgi.eba y.com/BR
01e0  4f 57 4e 2d 48 4f 42 4f  2d 55 4e 44 45 52 2d 54   OWN-HOBO -UNDER-T
01f0  48 45 2d 43 41 4e 4f 50  59 2d 4c 45 41 54 48 45   HE-CANOP Y-LEATHE
0200  52 2d 42 41 47 2d 42 41  43 4b 2d 50 41 43 4b 2d   R-BAG-BA CK-PACK-
0210  50 55 5f 57 30 51 51 69  74 65 6d 5a 32 33 30 32   PU_W0QQi temZ2302
0220  37 32 32 37 31 36 32 31  51 51 69 68 5a 30 31 33   72271621 QQihZ013
0230  51 51 63 61 74 65 67 6f  72 79 5a 36 33 38 35 32   QQcatego ryZ63852
0240  51 51 73 73 50 61 67 65  4e 61 6d 65 5a 57 44 56   QQssPage NameZWDV
0250  57 51 51 72 64 5a 31 51  51 63 6d 64 5a 56 69 65   WQQrdZ1Q QcmdZVie
0260  77 49 74 65 6d 0d 0a 0d  0a c8 82 bb 93            wItem··· ·····
```

Figure 6

3) Locate the email traffic you want to extract. Right-click on the email traffic and select

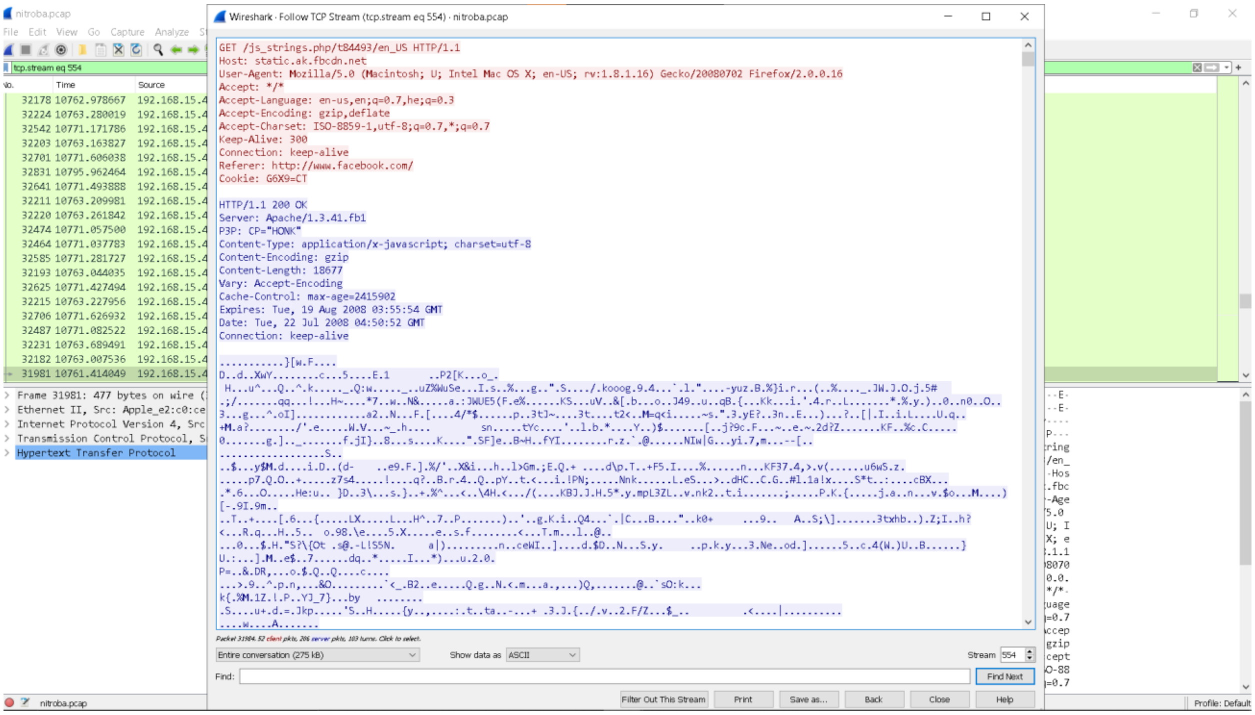
"Follow" > "TCP Stream". A new window will open displaying the entire email message. You can then copy and paste the email message into a text editor or email client.(in figure 7)



```
No.   Time         Source          Destination     Protocol Length Info
94847 15612.644030 192.168.15.4    69.22.167.246   HTTP      620 GET /aw/pics/vit/antiques2/ftr1_antiques2.gif HTTP/1.1
94844 15612.641508 69.22.167.246   192.168.15.4    HTTP     1091 HTTP/1.1 200 OK  (GIF89a)
94838 15612.624542 192.168.15.4    69.22.167.246   HTTP      622 GET /aw/pics/vit/antiques2/right2_antiques2.gif HTTP/1.1
94835 15612.621928 69.22.167.246   192.168.15.4    HTTP      318 HTTP/1.1 200 OK  (GIF89a)
94830 15612.615575 192.168.15.4    69.22.167.24                  it/antiques2/left2_antiques2.gif HTTP/1.1
94827 15612.612703 69.22.167.246   192.168.15.4                  <  (GIF89a)
94819 15612.562109 192.168.15.4    69.22.167.24                  it/antiques2/right1bkgd_antiques2.gif HTTP/1.1
94818 15612.561331 192.168.15.4    69.22.167.24                  it/antiques2/right1_antiques2.gif HTTP/1.1
94816 15612.522787 72.21.202.98    192.168.15.4                  <  (JPEG JFIF image)
94804 15612.461129 69.22.167.246   192.168.15.4                  <  (GIF89a)
94796 15612.436144 69.22.167.246   192.168.15.4                  <  (GIF89a)
94794 15612.435328 192.168.15.4    69.22.167.24                  it/antiques2/left1bkgd_antiques2.gif HTTP/1.1
94790 15612.431567 69.22.167.246   192.168.15.4                  <  (GIF89a)
94779 15612.395382 38.102.35.231   192.168.15.4                  <  (GIF89a)
94777 15612.369138 192.168.15.4    69.22.167.24                  it/antiques2/hdr2bkgd_antiques2.gif HTTP/1.1
94776 15612.368738 192.168.15.4    38.102.35.23                  size/default.gif HTTP/1.1
94773 15612.365816 192.168.15.4    69.22.167.24                  it/antiques2/hdr1bkgd_antiques2.gif HTTP/1.1
94770 15612.363853 69.22.167.246   192.168.15.4
94769 15612.362238 69.22.167.246   192.168.15.4
94752 15612.331653 192.168.15.4    69.22.167.24                  f HTTP/1.1
94749 15612.328901 69.22.167.246   192.168.15.4
94748 15612.325696 192.168.15.4    69.22.167.24                  HTTP/1.1
94736 15612.299997 192.168.15.4    72.21.202.98                  pg HTTP/1.1
94733 15612.297445 192.168.15.4    69.22.167.246   HTTP      620 GET /aw/pics/v          HTTP/1.1
94730 15612.289885 69.22.167.246   192.168.15.4    HTTP     1107 HTTP/1.1 200 C
94728 15612.272576 192.168.15.4    69.22.167.246   HTTP      615 GET /aw/pics/i          /1.1
94703 15603.219423 216.113.185.92  192.168.15.4    HTTP     1448 Continuation
94692 15603.068416 76.13.212.11    192.168.15.4    HTTP      775 HTTP/1.1 200 OK  (text/html)
94688 15602.909143 66.211.160.61   192.168.15.4    HTTP     1298 HTTP/1.1 200 OK  (JPEG JFIF image)
94672 15602.705917 66.94.234.72    192.168.15.4    HTTP      481 HTTP/1.1 200 OK  (GIF89a)
94667 15602.695833 66.94.234.72    192.168.15.4    HTTP      481 HTTP/1.1 200 OK  (GIF89a)
94664 15602.691744 192.168.15.4    66.94.234.72    HTTP      359 GET /b?P=0WnyqNj8fU8jASHXQnAf7GNERoZbDEiFehUACHM5&T=18g463mdb%2fX%3d1216707093%2fE%3d97553668%2fR%3deb_cmptr%2fK%3d5%2fV%3d8.1…
94662 15602.681556 192.168.15.4    66.94.234.72    HTTP      355 GET /b?P=O1AuiNj8fU8jASHXQnAf7IwgRoZbDEiFehUAB_bG&T=18ae97hds%2fX%3d1216707093%2fE%3d97553668%2fR%3deb_cmptr%2fK%3d5%2fV%3d8.1…
94659 15602.656880 66.211.160.22   192.168.15.4    HTTP     1133 HTTP/1.1 200 OK  (JPEG JFIF image)
94656 15602.594891 192.168.15.4    66.211.160.22   HTTP      588 GET /pict/1102715400118080_1.jpg HTTP/1.1
94654 15602.592777 66.211.160.22   192.168.15.4    HTTP     1292 HTTP/1.1 200 OK  (JPEG JFIF image)
94651 15602.540875 192.168.15.4    66.211.160.22   HTTP      588 GET /pict/3002417858698080_1.jpg HTTP/1.1
94649 15602.533140 66.211.160.22   192.168.15.4    HTTP     1292 HTTP/1.1 200 OK  (JPEG JFIF image)
94646 15602.472369 192.168.15.4    66.211.160.22   HTTP      588 GET /pict/3800463069298080_1.jpg HTTP/1.1
94644 15602.469947 66.211.160.22   192.168.15.4    HTTP     1293 HTTP/1.1 200 OK  (JPEG JFIF image)
```

Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comments
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
DCCP Stream Ctrl+Alt+Shift+E
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H
HTTP/2 Stream
QUIC Stream
SIP Call

Figure 7



nitroba.pcap
File Edit View Go Capture Analyze St
tcp.stream eq 554
Wireshark · Follow TCP Stream (tcp.stream eq 554) · nitroba.pcap

```
No.   Time         Source
32178 10762.978667 192.168.15.4
32224 10763.280019 192.168.15.4
32542 10771.171786 192.168.15.4
32203 10763.163827 192.168.15.4
32701 10771.606038 192.168.15.4
32831 10795.962464 192.168.15.4
32641 10771.493888 192.168.15.4
32211 10763.209981 192.168.15.4
32220 10763.261842 192.168.15.4
32474 10771.057500 192.168.15.4
32464 10771.037783 192.168.15.4
32585 10771.281727 192.168.15.4
32193 10763.044035 192.168.15.4
32625 10771.427494 192.168.15.4
32215 10763.227956 192.168.15.4
32706 10771.626932 192.168.15.4
32487 10771.082522 192.168.15.4
32231 10763.689491 192.168.15.4
32182 10763.007536 192.168.15.4
31981 10761.414049 192.168.15.4

> Frame 31981: 477 bytes on wire (
> Ethernet II, Src: Apple_e2:c0:ce
> Internet Protocol Version 4, Src
> Transmission Control Protocol, S
> Hypertext Transfer Protocol
```

```
GET /js_strings.php/t84493/en_US HTTP/1.1
Host: static.ak.fbcdn.net
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X; en-US; rv:1.8.1.16) Gecko/20080702 Firefox/2.0.0.16
Accept: */*
Accept-Language: en-us,en;q=0.7,he;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.facebook.com/
Cookie: G6X9=CT

HTTP/1.1 200 OK
Server: Apache/1.3.41.fb1
P3P: CP="HONK"
Content-Type: application/x-javascript; charset=utf-8
Content-Encoding: gzip
Content-Length: 18677
Vary: Accept-Encoding
Cache-Control: max-age=2415902
Expires: Tue, 19 Aug 2008 03:55:54 GMT
Date: Tue, 22 Jul 2008 04:50:52 GMT
Connection: keep-alive

...........}[w.F....
D..d..XwY........c...5....E.1       ..P2[K...o_.
 H...u^...Q..^.k....._.Q:w....._..uZ%WuSe...I.s..%...g..".S..../.kooog.9.4...`.l."....-yuz.B.%}i.r...(..%...._.JW.J.O.j.5#
.;/.......qq...!...H~....*7..w..N&.....a.:JWUE5(F.e%......KS...uV..&[.b...o..J49..u..qB.{...Kk...i.'.4.r..L.......*.%.y.)..0..n0..O..
3...g...^.oI]............a2..N...F.[....4/*$......p..3t]~....3t....t2<..M=q<i.....~s.".3.yE?..3n..E...)...?..[|.I..i.L....U.q..
+M.a?......../'.e.....W.V...~_.h....         sn.....tYc....'..l.b.*....Y..)$.......[..j?9c.F...~..e.~.2d?Z.......KF..%c.C.....
0.......g.].._.......f.jI}..8...s....K....".SF]e..B~H..fYI........r.z.`.@......NIw|G...yi.7,m...--[..
..................S..
..$...y$M.d....i.D..(d-    ..e9.F.].%/'..X&i...h..l>Gm.;E.Q.+ ....d\p.T..+F5.I....%......n...KF37.4,>.v(......u6wS.z.
.....p7.Q.O..+.....z7s4.....!....q?..B.r.4..Q..pY..t.<...i.!PN;.....Nnk......L.eS...>..dHC..C.G..#l.1a!x....S*t..:....cBX...
.*.6...O.....He:u.. }D..3\...s.}..+.%^...<..\4H.<.../(....KBJ.J.H.5*.y.mpL3ZL..v.nk2..t.i.......;.....P.K.{.....j.a..n...v.$o...M....)
[-.9I.9m..
..T..+....[.6...{.....LX.....L...H^..7..P.......)..'..g.K.i..Q4...`.|C...B....."..k0+     ...9..   A..S;\].......3txhb..).Z;I..h?
<...R.q...H..5..  o.98.\e....5.X.....e..s.f........<...T.m...l..@..
...0...$.H."S?\{Ot .s@.-L!S5N.      a|).........n..ceWI..]....d.$D..N...S.y.     ..p.k.y...3.Ne..od.]......5..c.4(W.)U..B......}
U.:...].M..e$..7......dq..*.....I...*)...u.2.0.
P=..&.DR,...o.$.Q..Q....c....
...>.9..^.p.n,...&O.........`<_.B2..e.....Q.g..N.<.m...a.,...)Q,.......@..`sO:k...
k{.%M.1Z.!.P..YJ_7}...by  ........
.S....u+.d.=.Jkp.....'S..H.....{y..,....:.t..ta..-...+ .3.J.{../.v..2.F/Z...$_..        .<....|.........
....w....A.......
```

Packet 31984. 52 client pkts, 286 server pkts, 103 turns. Click to select.

4)To extract all HTTP contents from the pcap file, you can use Wireshark's "Export Objects" feature.

5)Click on "File" > "Export Objects" > "HTTP". (in figure 8)

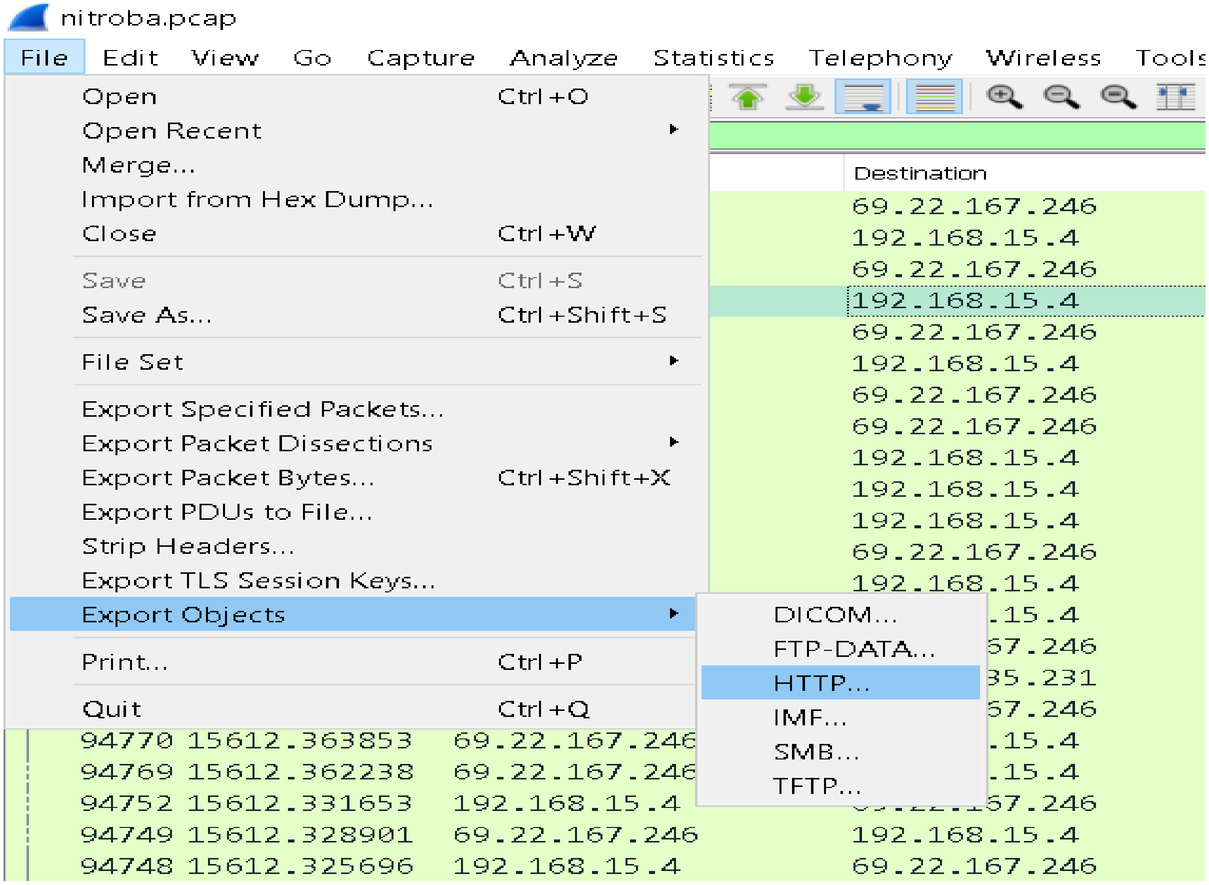
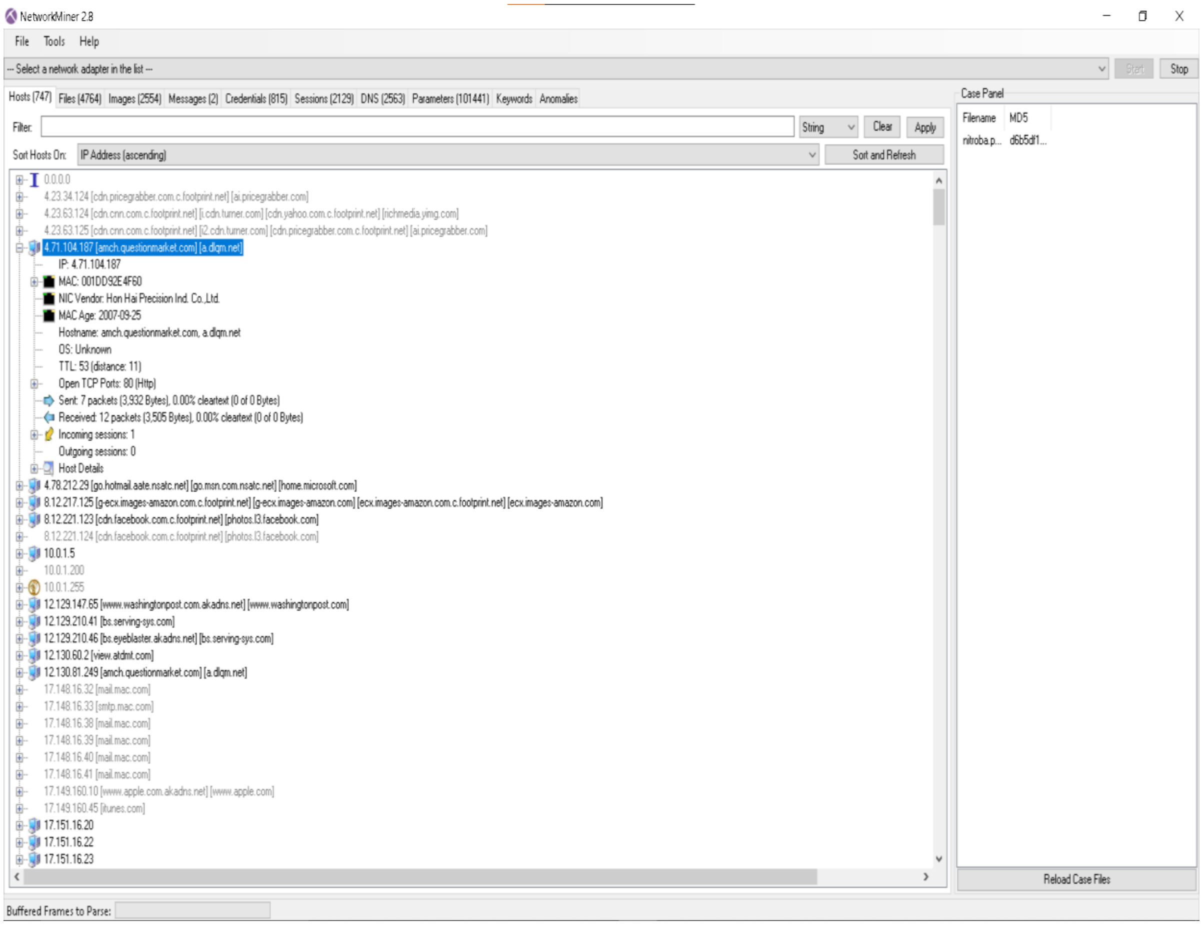


Figure 8

6) Wireshark will then extract all HTTP objects from the pcap file and save them to a directory of your choice.

NETWORK MINER

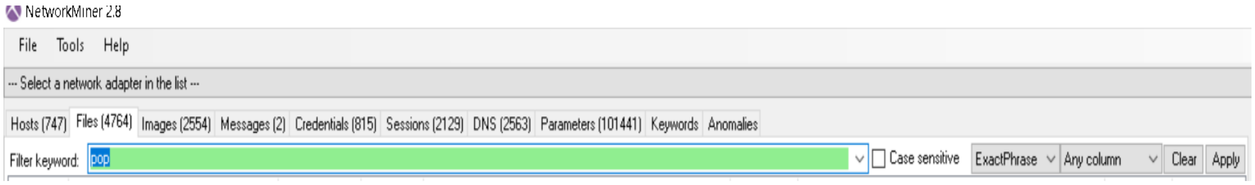
1) upload the file in the file section of the network miner so we can get the detailed division of the packets



Filename	MD5
nitroba.p...	d6b5df1...

```
0.0.0.0
4.23.34.124 [cdn.pricegrabber.com.c.footprint.net] [ai.pricegrabber.com]
4.23.63.124 [cdn.cnn.com.c.footprint.net] [i.cdn.turner.com] [cdn.yahoo.com.c.footprint.net] [richmedia.yimg.com]
4.23.63.125 [cdn.cnn.com.c.footprint.net] [i2.cdn.turner.com] [cdn.pricegrabber.com.c.footprint.net] [ai.pricegrabber.com]
4.71.104.187 [amch.questionmarket.com] [a.dlqm.net]
    IP: 4.71.104.187
    MAC: 001DD92E4F60
    NIC Vendor: Hon Hai Precision Ind. Co.,Ltd.
    MAC Age: 2007-09-25
    Hostname: amch.questionmarket.com, a.dlqm.net
    OS: Unknown
    TTL: 53 (distance: 11)
    Open TCP Ports: 80 (Http)
    Sent: 7 packets (3,932 Bytes), 0.00% cleartext (0 of 0 Bytes)
    Received: 12 packets (3,505 Bytes), 0.00% cleartext (0 of 0 Bytes)
    Incoming sessions: 1
    Outgoing sessions: 0
    Host Details
4.78.212.29 [go.hotmail.aate.nsatc.net] [go.msn.com.nsatc.net] [home.microsoft.com]
8.12.217.125 [g-ecx.images-amazon.com.c.footprint.net] [g-ecx.images-amazon.com] [ecx.images-amazon.com.c.footprint.net] [ecx.images-amazon.com]
8.12.221.123 [cdn.facebook.com.c.footprint.net] [photos.l3.facebook.com]
8.12.221.124 [cdn.facebook.com.c.footprint.net] [photos.l3.facebook.com]
10.0.1.5
10.0.1.200
10.0.1.255
12.129.147.65 [www.washingtonpost.com.akadns.net] [www.washingtonpost.com]
12.129.210.41 [bs.serving-sys.com]
12.129.210.46 [bs.eyeblaster.akadns.net] [bs.serving-sys.com]
12.130.60.2 [view.atdmt.com]
12.130.81.249 [amch.questionmarket.com] [a.dlqm.net]
17.148.16.32 [mail.mac.com]
17.148.16.33 [smtp.mac.com]
17.148.16.38 [mail.mac.com]
17.148.16.39 [mail.mac.com]
17.148.16.40 [mail.mac.com]
17.148.16.41 [mail.mac.com]
17.149.160.10 [www.apple.com.akadns.net] [www.apple.com]
17.149.160.45 [itunes.com]
17.151.16.20
17.151.16.22
17.151.16.23
```

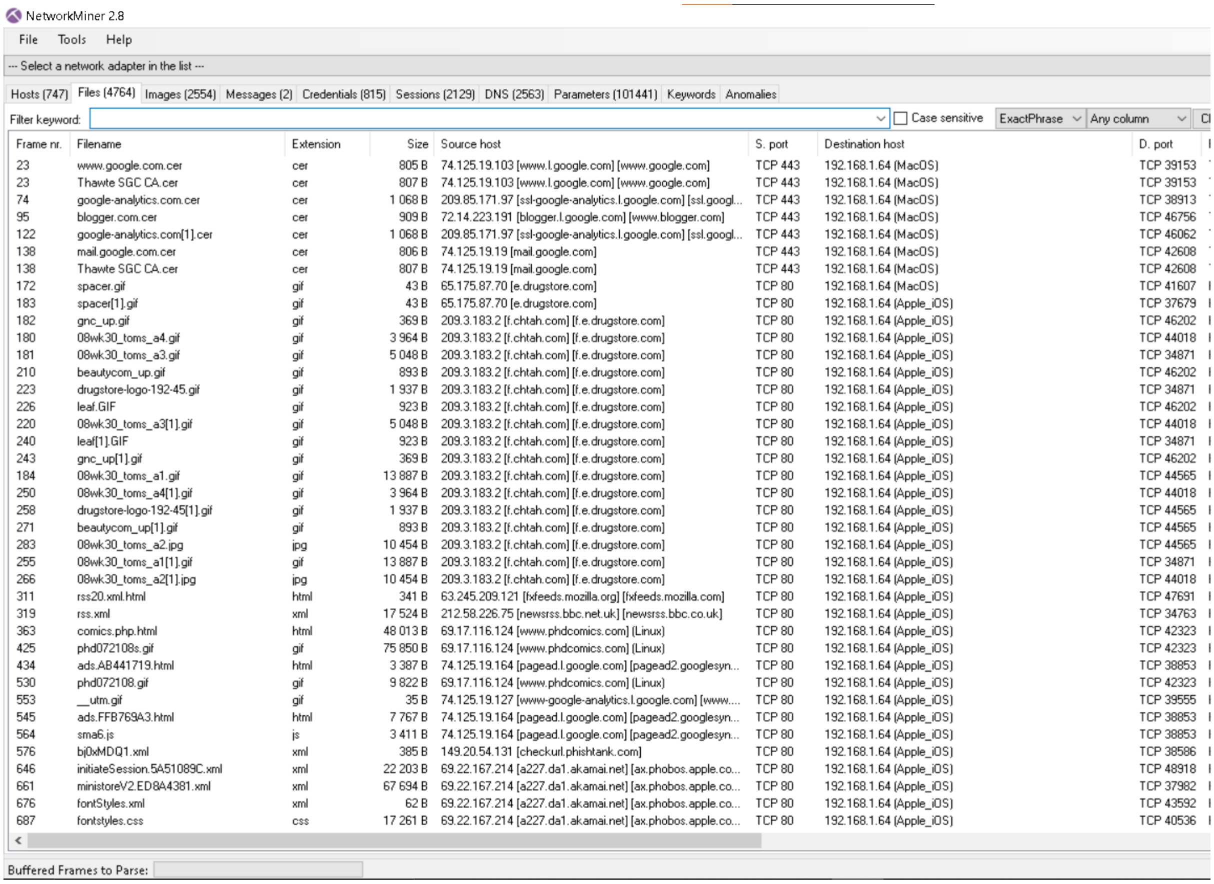
In this host section, we can get the Ip address, hostname, and mail.



Filter keyword: pop

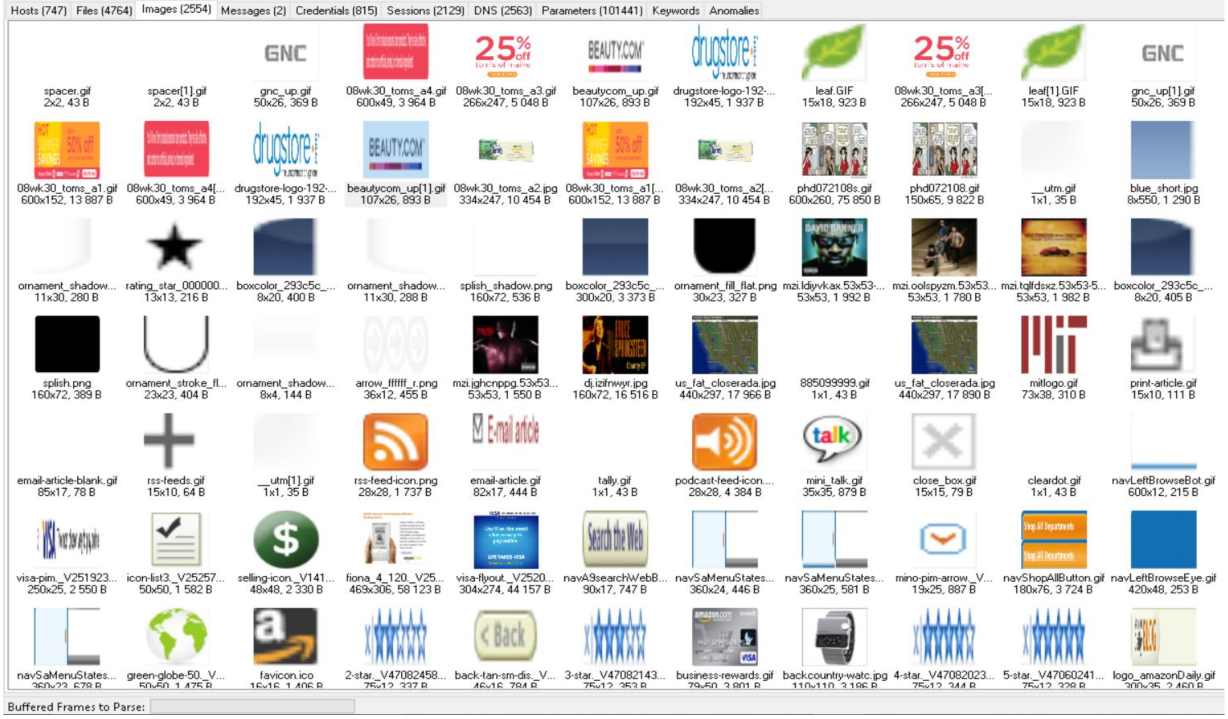
□ Case sensitive

2)We can get all the content in the .pcap file we can filter the type of protocols in the files section

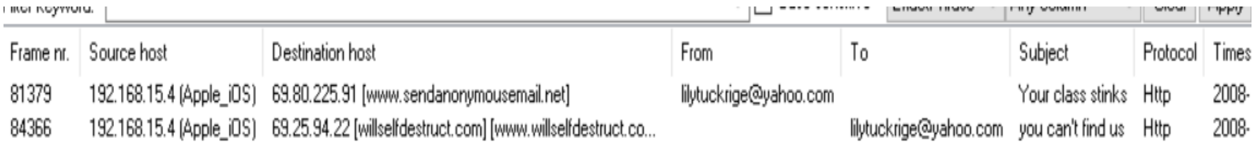


Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host	D. port
23	www.google.com.cer	cer	805 B	74.125.19.103 [www.l.google.com] [www.google.com]	TCP 443	192.168.1.64 (MacOS)	TCP 39153
23	Thawte SGC CA.cer	cer	807 B	74.125.19.103 [www.l.google.com] [www.google.com]	TCP 443	192.168.1.64 (MacOS)	TCP 39153
74	google-analytics.com.cer	cer	1 068 B	209.85.171.97 [ssl-google-analytics.l.google.com] [ssl.googl...	TCP 443	192.168.1.64 (MacOS)	TCP 38913
95	blogger.com.cer	cer	909 B	72.14.223.191 [blogger.l.google.com] [www.blogger.com]	TCP 443	192.168.1.64 (MacOS)	TCP 46756
122	google-analytics.com[1].cer	cer	1 068 B	209.85.171.97 [ssl-google-analytics.l.google.com] [ssl.googl...	TCP 443	192.168.1.64 (MacOS)	TCP 46062
138	mail.google.com.cer	cer	806 B	74.125.19.19 [mail.google.com]	TCP 443	192.168.1.64 (MacOS)	TCP 42608
138	Thawte SGC CA.cer	cer	807 B	74.125.19.19 [mail.google.com]	TCP 443	192.168.1.64 (MacOS)	TCP 42608
172	spacer.gif	gif	43 B	65.175.87.70 [e.drugstore.com]	TCP 80	192.168.1.64 (MacOS)	TCP 41607
183	spacer[1].gif	gif	43 B	65.175.87.70 [e.drugstore.com]	TCP 80	192.168.1.64 (Apple_iOS)	TCP 37679
182	gnc_up.gif	gif	369 B	209.3.183.2 [f.chtah.com] [f.e.drugstore.com]	TCP 80	192.168.1.64 (Apple_iOS)	TCP 46202
180	08wk30_toms_a4.gif	gif	3 964 B	209.3.183.2 [f.chtah.com] [f.e.drugstore.com]	TCP 80	192.168.1.64 (Apple_iOS)	TCP 44018
181	08wk30_toms_a3.gif	gif	5 048 B	209.3.183.2 [f.chtah.com] [f.e.drugstore.com]	TCP 80	192.168.1.64 (Apple_iOS)	TCP 34871
210	beautycom_up.gif	gif	893 B	209.3.183.2 [f.chtah.com] [f.e.drugstore.com]	TCP 80	192.168.1.64 (Apple_iOS)	TCP 46202
223	drugstore-logo-192-45.gif	gif	1 937 B	209.3.183.2 [f.chtah.com] [f.e.drugstore.com]	TCP 80	192.168.1.64 (Apple_iOS)	TCP 34871
226	leaf.GIF	gif	923 B	209.3.183.2 [f.chtah.com] [f.e.drugstore.com]	TCP 80	192.168.1.64 (Apple_iOS)	TCP 46202
220	08wk30_toms_a3[1].gif	gif	5 048 B	209.3.183.2 [f.chtah.com] [f.e.drugstore.com]	TCP 80	192.168.1.64 (Apple_iOS)	TCP 44018
240	leaf[1].GIF	gif	923 B	209.3.183.2 [f.chtah.com] [f.e.drugstore.com]	TCP 80	192.168.1.64 (Apple_iOS)	TCP 34871
243	gnc_up[1].gif	gif	369 B	209.3.183.2 [f.chtah.com] [f.e.drugstore.com]	TCP 80	192.168.1.64 (Apple_iOS)	TCP 46202
184	08wk30_toms_a1.gif	gif	13 887 B	209.3.183.2 [f.chtah.com] [f.e.drugstore.com]	TCP 80	192.168.1.64 (Apple_iOS)	TCP 44565
250	08wk30_toms_a4[1].gif	gif	3 964 B	209.3.183.2 [f.chtah.com] [f.e.drugstore.com]	TCP 80	192.168.1.64 (Apple_iOS)	TCP 44018
258	drugstore-logo-192-45[1].gif	gif	1 937 B	209.3.183.2 [f.chtah.com] [f.e.drugstore.com]	TCP 80	192.168.1.64 (Apple_iOS)	TCP 44565
271	beautycom_up[1].gif	gif	893 B	209.3.183.2 [f.chtah.com] [f.e.drugstore.com]	TCP 80	192.168.1.64 (Apple_iOS)	TCP 44565
283	08wk30_toms_a2.jpg	jpg	10 454 B	209.3.183.2 [f.chtah.com] [f.e.drugstore.com]	TCP 80	192.168.1.64 (Apple_iOS)	TCP 44565
255	08wk30_toms_a1[1].gif	gif	13 887 B	209.3.183.2 [f.chtah.com] [f.e.drugstore.com]	TCP 80	192.168.1.64 (Apple_iOS)	TCP 34871
266	08wk30_toms_a2[1].jpg	jpg	10 454 B	209.3.183.2 [f.chtah.com] [f.e.drugstore.com]	TCP 80	192.168.1.64 (Apple_iOS)	TCP 44018
311	rss20.xml.html	html	341 B	63.245.209.121 [fxfeeds.mozilla.org] [fxfeeds.mozilla.com]	TCP 80	192.168.1.64 (Apple_iOS)	TCP 47691
319	rss.xml	xml	17 524 B	212.58.226.75 [newsrss.bbc.net.uk] [newsrss.bbc.co.uk]	TCP 80	192.168.1.64 (Apple_iOS)	TCP 34763
363	comics.php.html	html	48 013 B	69.17.116.124 [www.phdcomics.com] (Linux)	TCP 80	192.168.1.64 (Apple_iOS)	TCP 42323
425	phd072108s.gif	gif	75 850 B	69.17.116.124 [www.phdcomics.com] (Linux)	TCP 80	192.168.1.64 (Apple_iOS)	TCP 42323
434	ads.AB441719.html	html	3 387 B	74.125.19.164 [pagead.l.google.com] [pagead2.googlesyn...	TCP 80	192.168.1.64 (Apple_iOS)	TCP 38853
530	phd072108.gif	gif	9 822 B	69.17.116.124 [www.phdcomics.com] (Linux)	TCP 80	192.168.1.64 (Apple_iOS)	TCP 42323
553	__utm.gif	gif	35 B	74.125.19.127 [www-google-analytics.l.google.com] [www....	TCP 80	192.168.1.64 (Apple_iOS)	TCP 39555
545	ads.FFB769A3.html	html	7 767 B	74.125.19.164 [pagead.l.google.com] [pagead2.googlesyn...	TCP 80	192.168.1.64 (Apple_iOS)	TCP 38853
564	sma6.js	js	3 411 B	74.125.19.164 [pagead.l.google.com] [pagead2.googlesyn...	TCP 80	192.168.1.64 (Apple_iOS)	TCP 38853
576	bj0xMDQ1.xml	xml	385 B	149.20.54.131 [checkurl.phishtank.com]	TCP 80	192.168.1.64 (Apple_iOS)	TCP 38586
646	initiateSession.5A51089C.xml	xml	22 203 B	69.22.167.214 [a227.da1.akamai.net] [ax.phobos.apple.co...	TCP 80	192.168.1.64 (Apple_iOS)	TCP 48918
661	ministoreV2.ED8A4381.xml	xml	67 694 B	69.22.167.214 [a227.da1.akamai.net] [ax.phobos.apple.co...	TCP 80	192.168.1.64 (Apple_iOS)	TCP 37982
676	fontStyles.xml	xml	62 B	69.22.167.214 [a227.da1.akamai.net] [ax.phobos.apple.co...	TCP 80	192.168.1.64 (Apple_iOS)	TCP 43592
687	fontstyles.css	css	17 261 B	69.22.167.214 [a227.da1.akamai.net] [ax.phobos.apple.co...	TCP 80	192.168.1.64 (Apple_iOS)	TCP 40536

3)And images in the images section

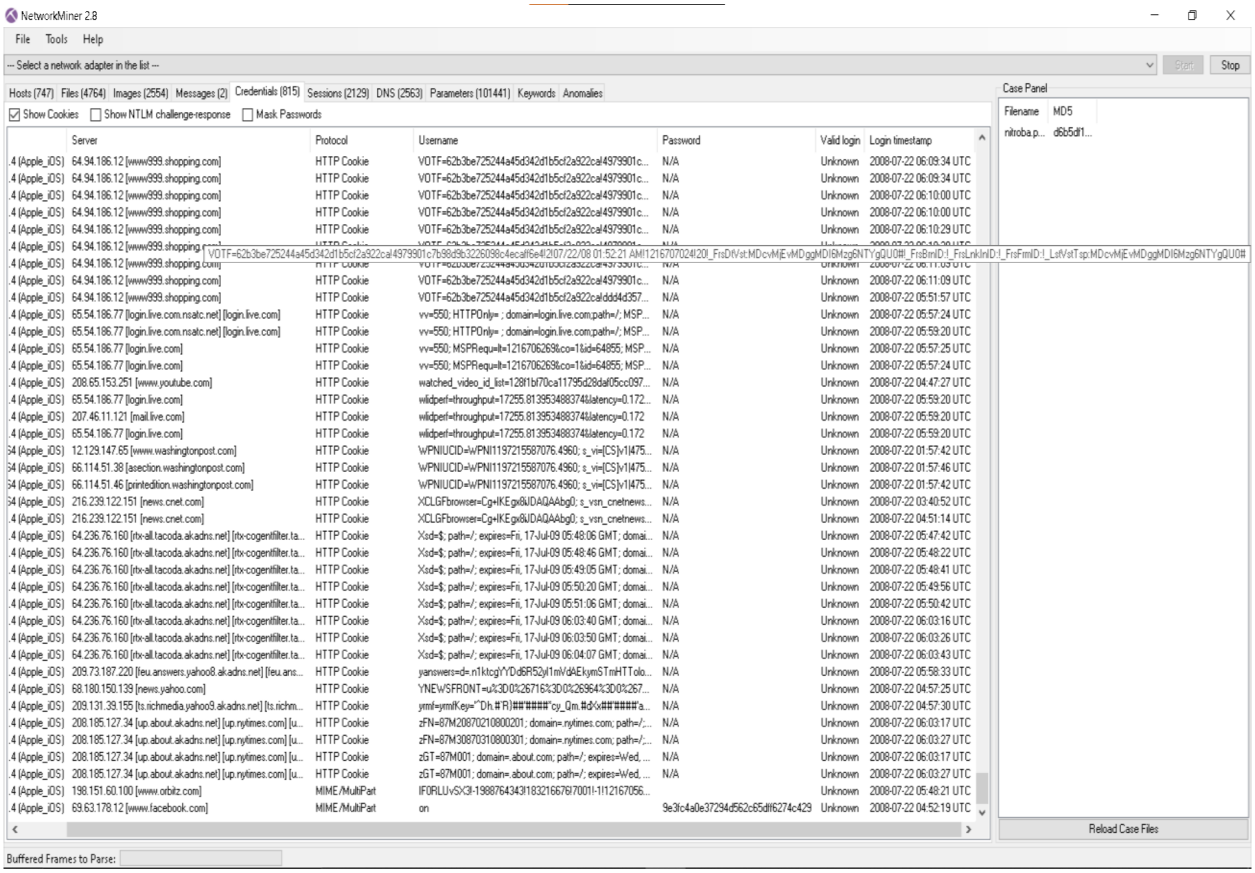

Hosts (747)
Files (4764)
Images (2554)
Messages (2)
Credentials (815)
Sessions (2129)
DNS (2563)
Parameters (101441)
Keywords
Anomalies
spacer.gif 2x2, 43 B
spacer[1].gif 2x2, 43 B
gnc_up.gif 50x26, 369 B
08wk30_toms_a4.gif 600x49, 3 964 B
08wk30_toms_a3.gif 266x247, 5 048 B
beautycom_up.gif 107x26, 893 B
drugstore-logo-192-... 192x45, 1 937 B
leaf.GIF 15x18, 923 B
08wk30_toms_a3[... 266x247, 5 048 B
leaf[1].GIF 15x18, 923 B
gnc_up[1].gif 50x26, 369 B
08wk30_toms_a1.gif 600x152, 13 887 B
08wk30_toms_a4[... 600x49, 3 964 B
drugstore-logo-192-... 192x45, 1 937 B
beautycom_up[1].gif 107x26, 893 B
08wk30_toms_a2.jpg 334x247, 10 454 B
08wk30_toms_a1[... 600x152, 13 887 B
08wk30_toms_a2[... 334x247, 10 454 B
phd072108s.gif 600x260, 75 850 B
phd072108.gif 150x65, 9 822 B
__utm.gif 1x1, 35 B
blue_short.jpg 8x550, 1 290 B
ornament_shadow... 11x30, 280 B
rating_star_000000... 13x13, 216 B
boxcolor_293c5c_... 8x20, 400 B
ornament_shadow... 11x30, 288 B
splish_shadow.png 160x72, 536 B
boxcolor_293c5c_... 300x20, 3 373 B
ornament_fill_flat.png 30x23, 327 B
mzi.ldiyvkax.53x53-... 53x53, 1 992 B
mzi.oolspyzm.53x53... 53x53, 1 780 B
mzi.tqlfdsxz.53x53-5... 53x53, 1 982 B
boxcolor_293c5c_... 8x20, 405 B
splish.png 160x72, 389 B
ornament_stroke_fl... 23x23, 404 B
ornament_shadow... 8x4, 144 B
arrow_ffffff_r.png 36x12, 455 B
mzi.jghcnppg.53x53... 53x53, 1 550 B
dj.izifnwyr.jpg 160x72, 16 516 B
us_fat_closerada.jpg 440x297, 17 966 B
885099999.gif 1x1, 43 B
us_fat_closerada.jpg 440x297, 17 890 B
mitlogo.gif 73x38, 310 B
print-article.gif 15x10, 111 B
email-article-blank.gif 85x17, 78 B
rss-feeds.gif 15x10, 64 B
__utm[1].gif 1x1, 35 B
rss-feed-icon.png 28x28, 1 737 B
email-article.gif 82x17, 444 B
tally.gif 1x1, 43 B
podcast-feed-icon.... 28x28, 4 384 B
mini_talk.gif 35x35, 879 B
close_box.gif 15x15, 79 B
cleardot.gif 1x1, 43 B
navLeftBrowseBot.gif 600x12, 215 B
visa-pim._V251923... 250x25, 2 550 B
icon-list3._V25257... 50x50, 1 582 B
selling-icon._V141... 48x48, 2 330 B
fiona_4_120._V25... 469x306, 58 123 B
visa-flyout._V2520... 304x274, 44 157 B
navA9searchWebB... 90x17, 747 B
navSaMenuStates... 360x24, 446 B
navSaMenuStates... 360x25, 581 B
mino-pim-arrow._V... 19x25, 887 B
navShopAllButton.gif 180x76, 3 724 B
navLeftBrowseEye.gif 420x48, 253 B
navSaMenuStates... 360x23, 678 B
green-globe-50._V... 50x50, 1 475 B
favicon.ico 16x16, 1 406 B
2-star._V47082458... 75x12, 337 B
back-tan-sm-dis._V... 46x16, 784 B
3-star._V47082143... 75x12, 353 B
business-rewards.gif 79x50, 3 801 B
backcountry-watc.jpg 110x110, 3 186 B
4-star._V47082023... 75x12, 344 B
5-star._V47060241... 75x12, 328 B
logo_amazonDaily.gif 300x35, 2 460 B
Buffered Frames to Parse:

4) messages and VOIP calls in the messages section



Frame nr.	Source host	Destination host	From	To	Subject	Protocol	Times
81379	192.168.15.4 (Apple_iOS)	69.80.225.91 [www.sendanonymousemail.net]	lilytuckrige@yahoo.com		Your class stinks	Http	2008-
84366	192.168.15.4 (Apple_iOS)	69.25.94.22 [willselfdestruct.com] [www.willselfdestruct.co...		lilytuckrige@yahoo.com	you can't find us	Http	2008-

5) username and password in the credentials section



☑ Show Cookies ☐ Show NTLM challenge-response ☐ Mask Passwords

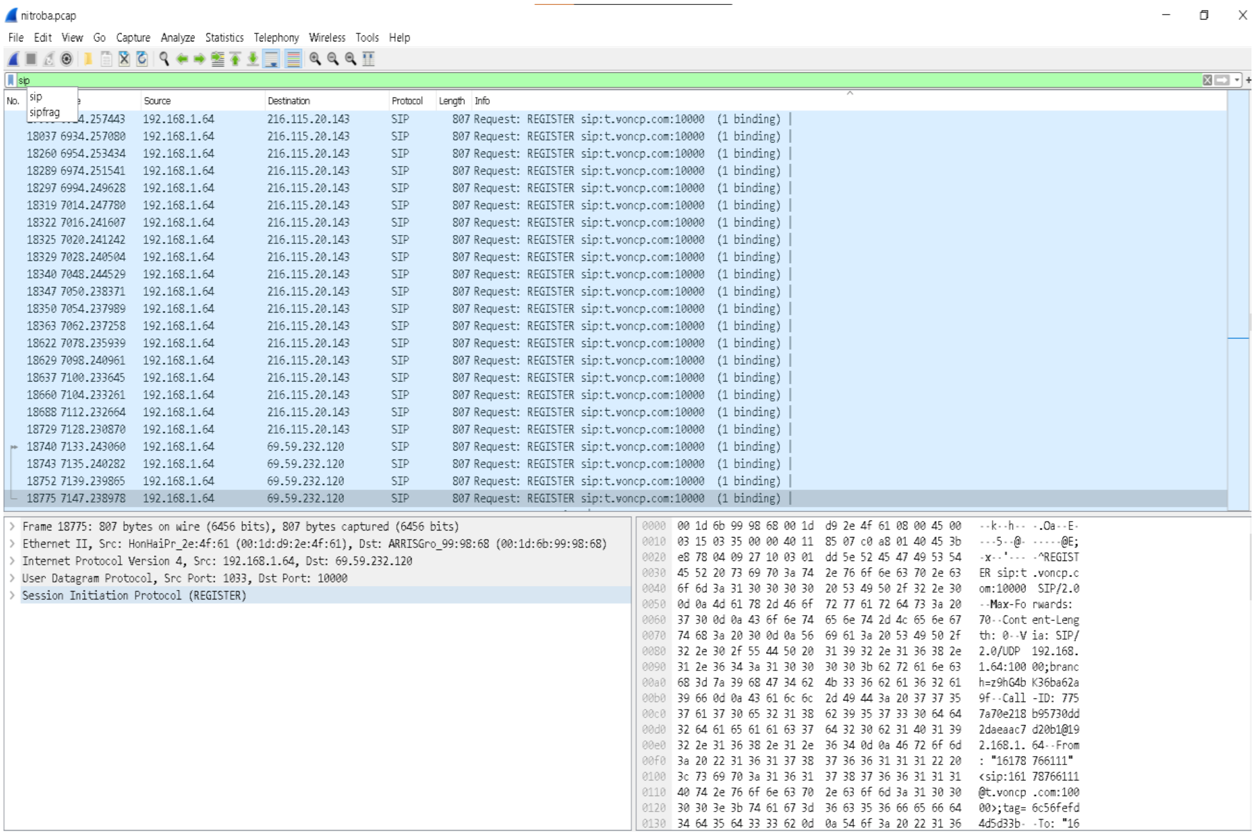
	Server	Protocol	Username	Password	Valid login	Login timestamp
.4 (Apple_iOS)	64.94.186.12 [www999.shopping.com]	HTTP Cookie	VOTF=62b3be725244a45d342d1b5cf2a922ca!4979901c...	N/A	Unknown	2008-07-22 06:09:34 UTC
.4 (Apple_iOS)	64.94.186.12 [www999.shopping.com]	HTTP Cookie	VOTF=62b3be725244a45d342d1b5cf2a922ca!4979901c...	N/A	Unknown	2008-07-22 06:09:34 UTC
.4 (Apple_iOS)	64.94.186.12 [www999.shopping.com]	HTTP Cookie	VOTF=62b3be725244a45d342d1b5cf2a922ca!4979901c...	N/A	Unknown	2008-07-22 06:10:00 UTC
.4 (Apple_iOS)	64.94.186.12 [www999.shopping.com]	HTTP Cookie	VOTF=62b3be725244a45d342d1b5cf2a922ca!4979901c...	N/A	Unknown	2008-07-22 06:10:00 UTC
.4 (Apple_iOS)	64.94.186.12 [www999.shopping.com]	HTTP Cookie	VOTF=62b3be725244a45d342d1b5cf2a922ca!4979901c...	N/A	Unknown	2008-07-22 06:10:29 UTC
.4 (Apple_iOS)	64.94.186.12 [www999.shopping.	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
.4 (Apple_iOS)	64.94.186.12 [www999.shopping.com]	HTTP Cookie	VOTF=62b3be725244a45d342d1b5cf2a922ca!4979901c...	N/A	Unknown	2008-07-22 06:11:09 UTC
.4 (Apple_iOS)	64.94.186.12 [www999.shopping.com]	HTTP Cookie	VOTF=62b3be725244a45d342d1b5cf2a922ca!4979901c...	N/A	Unknown	2008-07-22 06:11:09 UTC
.4 (Apple_iOS)	64.94.186.12 [www999.shopping.com]	HTTP Cookie	VOTF=62b3be725244a45d342d1b5cf2a922ca!ddd4d357...	N/A	Unknown	2008-07-22 05:51:57 UTC
.4 (Apple_iOS)	65.54.186.77 [login.live.com.nsatc.net] [login.live.com]	HTTP Cookie	vv=550; HTTPOnly= ; domain=login.live.com;path=/; MSP...	N/A	Unknown	2008-07-22 05:57:24 UTC
.4 (Apple_iOS)	65.54.186.77 [login.live.com.nsatc.net] [login.live.com]	HTTP Cookie	vv=550; HTTPOnly= ; domain=login.live.com;path=/; MSP...	N/A	Unknown	2008-07-22 05:59:20 UTC
.4 (Apple_iOS)	65.54.186.77 [login.live.com]	HTTP Cookie	vv=550; MSPRequ=lt=1216706269&co=1&id=64855; MSP...	N/A	Unknown	2008-07-22 05:57:25 UTC
.4 (Apple_iOS)	65.54.186.77 [login.live.com]	HTTP Cookie	vv=550; MSPRequ=lt=1216706269&co=1&id=64855; MSP...	N/A	Unknown	2008-07-22 05:57:24 UTC
.4 (Apple_iOS)	208.65.153.251 [www.youtube.com]	HTTP Cookie	watched_video_id_list=128f1bf70ca11795d28daf05cc097...	N/A	Unknown	2008-07-22 04:47:27 UTC
.4 (Apple_iOS)	65.54.186.77 [login.live.com]	HTTP Cookie	wlidperf=throughput=17255.813953488374&latency=0.172...	N/A	Unknown	2008-07-22 05:59:20 UTC
.4 (Apple_iOS)	207.46.11.121 [mail.live.com]	HTTP Cookie	wlidperf=throughput=17255.813953488374&latency=0.172	N/A	Unknown	2008-07-22 05:59:20 UTC
.4 (Apple_iOS)	65.54.186.77 [login.live.com]	HTTP Cookie	wlidperf=throughput=17255.813953488374&latency=0.172	N/A	Unknown	2008-07-22 05:59:20 UTC
54 (Apple_iOS)	12.129.147.65 [www.washingtonpost.com]	HTTP Cookie	WPNIUCID=WPNI1197215587076.4960; s_vi=[CS]v1|475...	N/A	Unknown	2008-07-22 01:57:42 UTC
54 (Apple_iOS)	66.114.51.38 [asection.washingtonpost.com]	HTTP Cookie	WPNIUCID=WPNI1197215587076.4960; s_vi=[CS]v1|475...	N/A	Unknown	2008-07-22 01:57:46 UTC
54 (Apple_iOS)	66.114.51.46 [printedition.washingtonpost.com]	HTTP Cookie	WPNIUCID=WPNI1197215587076.4960; s_vi=[CS]v1|475...	N/A	Unknown	2008-07-22 01:57:42 UTC
54 (Apple_iOS)	216.239.122.151 [news.cnet.com]	HTTP Cookie	XCLGFbrowser=Cg+IKEgx8iJDAQAAbg0; s_vsn_cnetnews...	N/A	Unknown	2008-07-22 03:40:52 UTC
.4 (Apple_iOS)	216.239.122.151 [news.cnet.com]	HTTP Cookie	XCLGFbrowser=Cg+IKEgx8iJDAQAAbg0; s_vsn_cnetnews...	N/A	Unknown	2008-07-22 04:51:14 UTC
.4 (Apple_iOS)	64.236.76.160 [rtx-all.tacoda.akadns.net] [rtx-cogentfilter.ta...	HTTP Cookie	Xsd=$; path=/; expires=Fri, 17-Jul-09 05:48:06 GMT; domai...	N/A	Unknown	2008-07-22 05:47:42 UTC
.4 (Apple_iOS)	64.236.76.160 [rtx-all.tacoda.akadns.net] [rtx-cogentfilter.ta...	HTTP Cookie	Xsd=$; path=/; expires=Fri, 17-Jul-09 05:48:46 GMT; domai...	N/A	Unknown	2008-07-22 05:48:22 UTC
.4 (Apple_iOS)	64.236.76.160 [rtx-all.tacoda.akadns.net] [rtx-cogentfilter.ta...	HTTP Cookie	Xsd=$; path=/; expires=Fri, 17-Jul-09 05:49:05 GMT; domai...	N/A	Unknown	2008-07-22 05:48:41 UTC
.4 (Apple_iOS)	64.236.76.160 [rtx-all.tacoda.akadns.net] [rtx-cogentfilter.ta...	HTTP Cookie	Xsd=$; path=/; expires=Fri, 17-Jul-09 05:50:20 GMT; domai...	N/A	Unknown	2008-07-22 05:49:56 UTC
.4 (Apple_iOS)	64.236.76.160 [rtx-all.tacoda.akadns.net] [rtx-cogentfilter.ta...	HTTP Cookie	Xsd=$; path=/; expires=Fri, 17-Jul-09 05:51:06 GMT; domai...	N/A	Unknown	2008-07-22 05:50:42 UTC
.4 (Apple_iOS)	64.236.76.160 [rtx-all.tacoda.akadns.net] [rtx-cogentfilter.ta...	HTTP Cookie	Xsd=$; path=/; expires=Fri, 17-Jul-09 06:03:40 GMT; domai...	N/A	Unknown	2008-07-22 06:03:16 UTC
.4 (Apple_iOS)	64.236.76.160 [rtx-all.tacoda.akadns.net] [rtx-cogentfilter.ta...	HTTP Cookie	Xsd=$; path=/; expires=Fri, 17-Jul-09 06:03:50 GMT; domai...	N/A	Unknown	2008-07-22 06:03:26 UTC
.4 (Apple_iOS)	64.236.76.160 [rtx-all.tacoda.akadns.net] [rtx-cogentfilter.ta...	HTTP Cookie	Xsd=$; path=/; expires=Fri, 17-Jul-09 06:04:07 GMT; domai...	N/A	Unknown	2008-07-22 06:03:43 UTC
.4 (Apple_iOS)	209.73.187.220 [feu.answers.yahoo8.akadns.net] [feu.ans...	HTTP Cookie	yanswers=d=.n1ktcgYYDd6R52yl1mVdAEkymSTmHTTolo...	N/A	Unknown	2008-07-22 05:58:33 UTC
.4 (Apple_iOS)	68.180.150.139 [news.yahoo.com]	HTTP Cookie	YNEWSFRONT=u%3D0%26716%3D0%26964%3D0%267...	N/A	Unknown	2008-07-22 04:57:25 UTC
.4 (Apple_iOS)	209.131.39.155 [ts.richmedia.yahoo9.akadns.net] [ts.richm...	HTTP Cookie	ymf=ymfKey="Dh.#'R}##'####"cy_Qm.#dXx##'####'a...	N/A	Unknown	2008-07-22 04:57:30 UTC
.4 (Apple_iOS)	208.185.127.34 [up.about.akadns.net] [up.nytimes.com] [u...	HTTP Cookie	zFN=87M20870210800201; domain=.nytimes.com; path=/;...	N/A	Unknown	2008-07-22 06:03:17 UTC
.4 (Apple_iOS)	208.185.127.34 [up.about.akadns.net] [up.nytimes.com] [u...	HTTP Cookie	zFN=87M30870310800301; domain=.nytimes.com; path=/;...	N/A	Unknown	2008-07-22 06:03:27 UTC
.4 (Apple_iOS)	208.185.127.34 [up.about.akadns.net] [up.nytimes.com] [u...	HTTP Cookie	zGT=87M001; domain=.about.com; path=/; expires=Wed, ...	N/A	Unknown	2008-07-22 06:03:17 UTC
.4 (Apple_iOS)	208.185.127.34 [up.about.akadns.net] [up.nytimes.com] [u...	HTTP Cookie	zGT=87M001; domain=.about.com; path=/; expires=Wed, ...	N/A	Unknown	2008-07-22 06:03:27 UTC
.4 (Apple_iOS)	198.151.60.100 [www.orbitz.com]	MIME/MultiPart	IF0RLUvSX3!-1988764343!183216676!7001!-1!12167056...		Unknown	2008-07-22 05:48:21 UTC
.4 (Apple_iOS)	69.63.178.12 [www.facebook.com]	MIME/MultiPart	on	9e3fc4a0e37294d562c65dff6274c429	Unknown	2008-07-22 04:52:19 UTC

VOTF=62b3be725244a45d342d1b5cf2a922ca!4979901c7b98d9b3226098c4ecaff6e4!2!07/22/08 01:52:21 AM!1216707024!20!_FrsDtVst:MDcvMjEvMDggMDI6Mzg6NTYgQU0#!_FrsBrnID:!_FrsLnkInID:!_FrsFrmID:!_LstVstTsp:MDcvMjEvMDggMDI6Mzg6NTYgQU0#

Filename	MD5
nitroba.p...	d6b5df1...

VOIP CALLS

1) To filter VoIP traffic, enter "sip" in the filter box at the top of the Wireshark window. This will display only SIP (Session Initiation Protocol) traffic, which is used to set up VoIP calls. (in figure 9)


nitroba.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
sip
sip
sipfrag

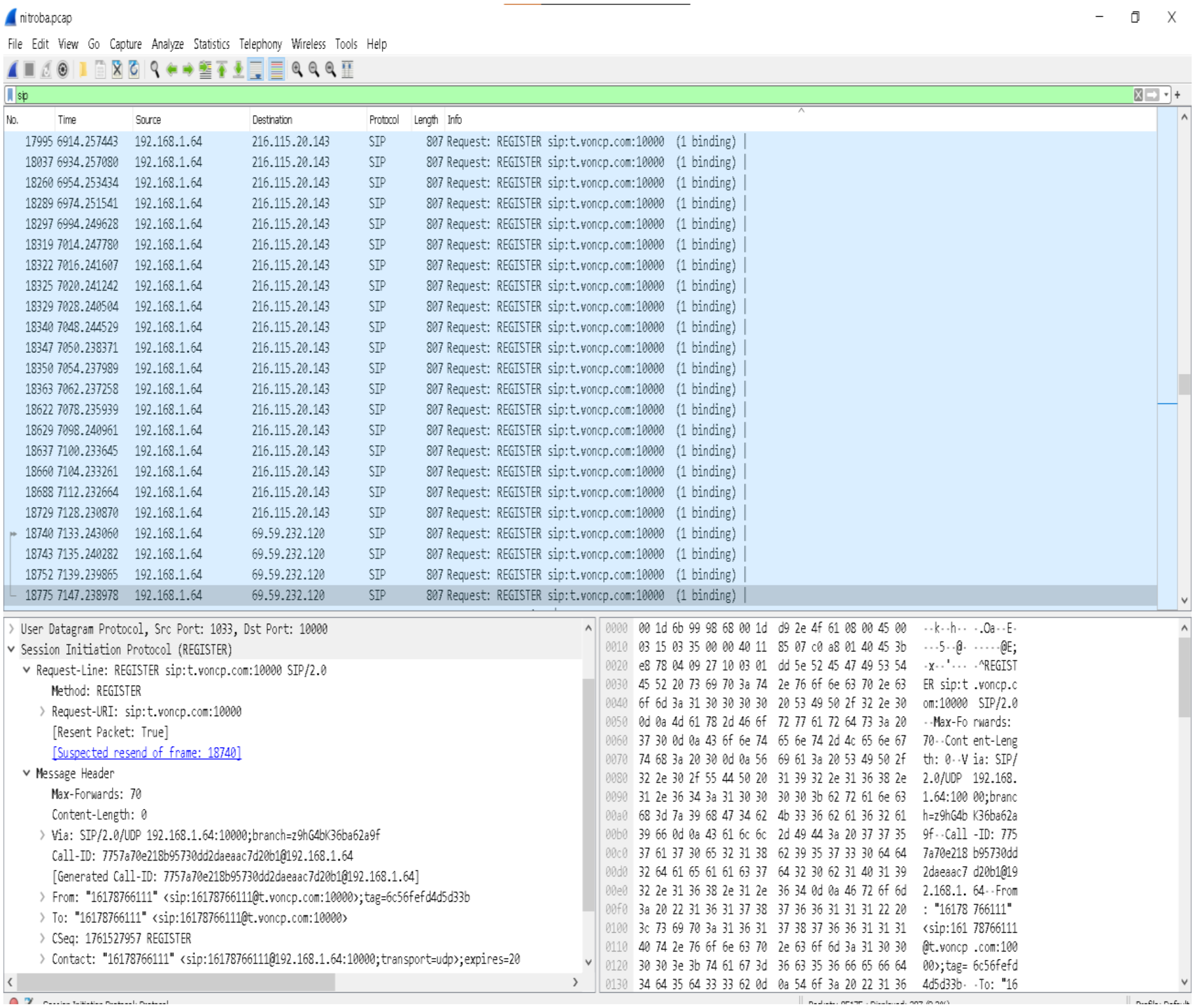
```
No.                 Source          Destination      Protocol  Length Info
      4.257443      192.168.1.64    216.115.20.143   SIP        807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
18037 6934.257080   192.168.1.64    216.115.20.143   SIP        807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
18260 6954.253434   192.168.1.64    216.115.20.143   SIP        807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
18289 6974.251541   192.168.1.64    216.115.20.143   SIP        807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
18297 6994.249628   192.168.1.64    216.115.20.143   SIP        807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
18319 7014.247780   192.168.1.64    216.115.20.143   SIP        807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
18322 7016.241607   192.168.1.64    216.115.20.143   SIP        807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
18325 7020.241242   192.168.1.64    216.115.20.143   SIP        807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
18329 7028.240504   192.168.1.64    216.115.20.143   SIP        807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
18340 7048.244529   192.168.1.64    216.115.20.143   SIP        807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
18347 7050.238371   192.168.1.64    216.115.20.143   SIP        807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
18350 7054.237989   192.168.1.64    216.115.20.143   SIP        807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
18363 7062.237258   192.168.1.64    216.115.20.143   SIP        807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
18622 7078.235939   192.168.1.64    216.115.20.143   SIP        807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
18629 7098.240961   192.168.1.64    216.115.20.143   SIP        807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
18637 7100.233645   192.168.1.64    216.115.20.143   SIP        807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
18660 7104.233261   192.168.1.64    216.115.20.143   SIP        807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
18688 7112.232664   192.168.1.64    216.115.20.143   SIP        807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
18729 7128.230870   192.168.1.64    216.115.20.143   SIP        807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
18740 7133.243060   192.168.1.64    69.59.232.120    SIP        807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
18743 7135.240282   192.168.1.64    69.59.232.120    SIP        807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
18752 7139.239865   192.168.1.64    69.59.232.120    SIP        807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
18775 7147.238978   192.168.1.64    69.59.232.120    SIP        807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
```

```
> Frame 18775: 807 bytes on wire (6456 bits), 807 bytes captured (6456 bits)
> Ethernet II, Src: HonHaiPr_2e:4f:61 (00:1d:d9:2e:4f:61), Dst: ARRISGro_99:98:68 (00:1d:6b:99:98:68)
> Internet Protocol Version 4, Src: 192.168.1.64, Dst: 69.59.232.120
> User Datagram Protocol, Src Port: 1033, Dst Port: 10000
> Session Initiation Protocol (REGISTER)
```

```
0000  00 1d 6b 99 98 68 00 1d  d9 2e 4f 61 08 00 45 00   ··k··h·· ·.Oa··E·
0010  03 15 03 35 00 00 40 11  85 07 c0 a8 01 40 45 3b   ···5··@· ·····@E;
0020  e8 78 04 09 27 10 03 01  dd 5e 52 45 47 49 53 54   ·x··'··· ·^REGIST
0030  45 52 20 73 69 70 3a 74  2e 76 6f 6e 63 70 2e 63   ER sip:t .voncp.c
0040  6f 6d 3a 31 30 30 30 30  20 53 49 50 2f 32 2e 30   om:10000  SIP/2.0
0050  0d 0a 4d 61 78 2d 46 6f  72 77 61 72 64 73 3a 20   ··Max-Fo rwards: 
0060  37 30 0d 0a 43 6f 6e 74  65 6e 74 2d 4c 65 6e 67   70··Cont ent-Leng
0070  74 68 3a 20 30 0d 0a 56  69 61 3a 20 53 49 50 2f   th: 0··V ia: SIP/
0080  32 2e 30 2f 55 44 50 20  31 39 32 2e 31 36 38 2e   2.0/UDP  192.168.
0090  31 2e 36 34 3a 31 30 30  30 30 3b 62 72 61 6e 63   1.64:100 00;branc
00a0  68 3d 7a 39 68 47 34 62  4b 33 36 62 61 36 32 61   h=z9hG4b K36ba62a
00b0  39 66 0d 0a 43 61 6c 6c  2d 49 44 3a 20 37 37 35   9f··Call -ID: 775
00c0  37 61 37 30 65 32 31 38  62 39 35 37 33 30 64 64   7a70e218 b95730dd
00d0  32 64 61 65 61 61 63 37  64 32 30 62 31 40 31 39   2daeaac7 d20b1@19
00e0  32 2e 31 36 38 2e 31 2e  36 34 0d 0a 46 72 6f 6d   2.168.1. 64··From
00f0  3a 20 22 31 36 31 37 38  37 36 36 31 31 31 22 20   : "16178 766111" 
0100  3c 73 69 70 3a 31 36 31  37 38 37 36 36 31 31 31   <sip:161 78766111
0110  40 74 2e 76 6f 6e 63 70  2e 63 6f 6d 3a 31 30 30   @t.voncp .com:100
0120  30 30 3e 3b 74 61 67 3d  36 63 35 36 66 65 66 64   00>;tag= 6c56fefd
0130  34 64 35 64 33 33 62 0d  0a 54 6f 3a 20 22 31 36   4d5d33b· ·To: "16
```

Figure 9

2) To view the contents of a VoIP call, select a SIP packet in the packet list pane and then expand the "Session Initiation Protocol" section in the packet details pane. Look for the "SDP (Session Description Protocol)" field, which contains information about the audio and video codecs used in the call. (in figure 10)



```
sip
```

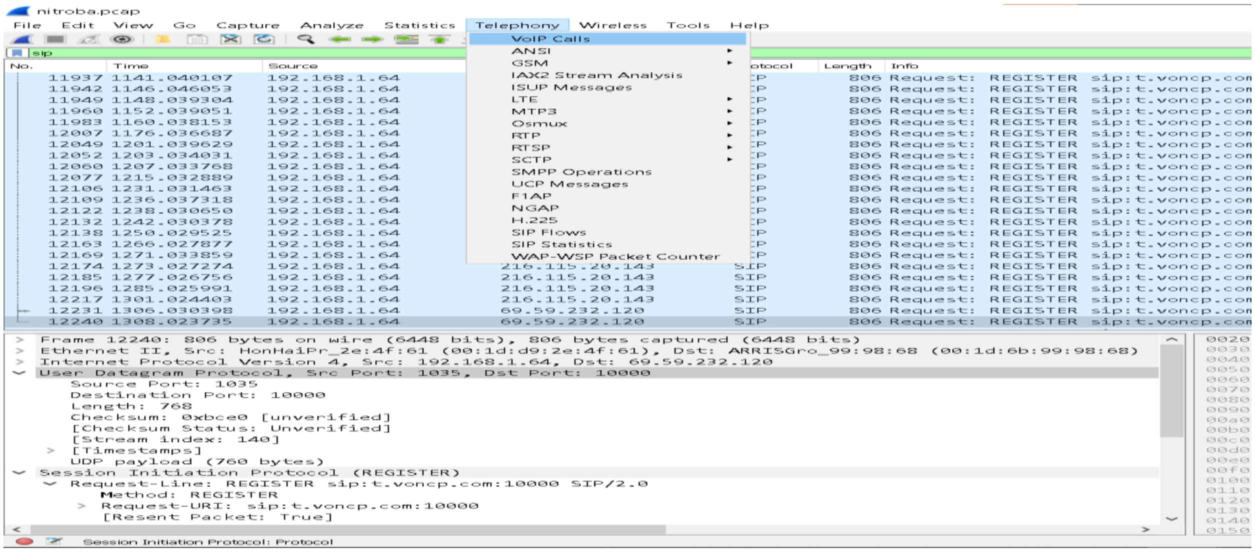
```
No.     Time          Source         Destination      Protocol  Length  Info
 17995 6914.257443   192.168.1.64   216.115.20.143   SIP       807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
 18037 6934.257080   192.168.1.64   216.115.20.143   SIP       807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
 18260 6954.253434   192.168.1.64   216.115.20.143   SIP       807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
 18289 6974.251541   192.168.1.64   216.115.20.143   SIP       807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
 18297 6994.249628   192.168.1.64   216.115.20.143   SIP       807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
 18319 7014.247780   192.168.1.64   216.115.20.143   SIP       807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
 18322 7016.241607   192.168.1.64   216.115.20.143   SIP       807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
 18325 7020.241242   192.168.1.64   216.115.20.143   SIP       807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
 18329 7028.240504   192.168.1.64   216.115.20.143   SIP       807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
 18340 7048.244529   192.168.1.64   216.115.20.143   SIP       807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
 18347 7050.238371   192.168.1.64   216.115.20.143   SIP       807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
 18350 7054.237989   192.168.1.64   216.115.20.143   SIP       807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
 18363 7062.237258   192.168.1.64   216.115.20.143   SIP       807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
 18622 7078.235939   192.168.1.64   216.115.20.143   SIP       807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
 18629 7098.240961   192.168.1.64   216.115.20.143   SIP       807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
 18637 7100.233645   192.168.1.64   216.115.20.143   SIP       807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
 18660 7104.233261   192.168.1.64   216.115.20.143   SIP       807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
 18688 7112.232664   192.168.1.64   216.115.20.143   SIP       807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
 18729 7128.230870   192.168.1.64   216.115.20.143   SIP       807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
 18740 7133.243060   192.168.1.64   69.59.232.120    SIP       807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
 18743 7135.240282   192.168.1.64   69.59.232.120    SIP       807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
 18752 7139.239865   192.168.1.64   69.59.232.120    SIP       807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
 18775 7147.238978   192.168.1.64   69.59.232.120    SIP       807 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
```

```
> User Datagram Protocol, Src Port: 1033, Dst Port: 10000
v Session Initiation Protocol (REGISTER)
  v Request-Line: REGISTER sip:t.voncp.com:10000 SIP/2.0
      Method: REGISTER
    > Request-URI: sip:t.voncp.com:10000
      [Resent Packet: True]
      [Suspected resend of frame: 18740]
  v Message Header
      Max-Forwards: 70
      Content-Length: 0
    > Via: SIP/2.0/UDP 192.168.1.64:10000;branch=z9hG4bK36ba62a9f
      Call-ID: 7757a70e218b95730dd2daeaac7d20b1@192.168.1.64
      [Generated Call-ID: 7757a70e218b95730dd2daeaac7d20b1@192.168.1.64]
    > From: "16178766111" <sip:16178766111@t.voncp.com:10000>;tag=6c56fefd4d5d33b
    > To: "16178766111" <sip:16178766111@t.voncp.com:10000>
    > CSeq: 1761527957 REGISTER
    > Contact: "16178766111" <sip:16178766111@192.168.1.64:10000;transport=udp>;expires=20
```

```
0000  00 1d 6b 99 98 68 00 1d  d9 2e 4f 61 08 00 45 00   ··k··h·· ·.Oa··E·
0010  03 15 03 35 00 00 40 11  85 07 c0 a8 01 40 45 3b   ···5··@· ·····@E;
0020  e8 78 04 09 27 10 03 01  dd 5e 52 45 47 49 53 54   ·x··'··· ·^REGIST
0030  45 52 20 73 69 70 3a 74  2e 76 6f 6e 63 70 2e 63   ER sip:t .voncp.c
0040  6f 6d 3a 31 30 30 30 30  20 53 49 50 2f 32 2e 30   om:10000  SIP/2.0
0050  0d 0a 4d 61 78 2d 46 6f  72 77 61 72 64 73 3a 20   ··Max-Fo rwards:
0060  37 30 0d 0a 43 6f 6e 74  65 6e 74 2d 4c 65 6e 67   70··Cont ent-Leng
0070  74 68 3a 20 30 0d 0a 56  69 61 3a 20 53 49 50 2f   th: 0··V ia: SIP/
0080  32 2e 30 2f 55 44 50 20  31 39 32 2e 31 36 38 2e   2.0/UDP  192.168.
0090  31 2e 36 34 3a 31 30 30  30 30 3b 62 72 61 6e 63   1.64:100 00;branc
00a0  68 3d 7a 39 68 47 34 62  4b 33 36 62 61 36 32 61   h=z9hG4b K36ba62a
00b0  39 66 0d 0a 43 61 6c 6c  2d 49 44 3a 20 37 37 35   9f··Call -ID: 775
00c0  37 61 37 30 65 32 31 38  62 39 35 37 33 30 64 64   7a70e218 b95730dd
00d0  32 64 61 65 61 61 63 37  64 32 30 62 31 40 31 39   2daeaac7 d20b1@19
00e0  32 2e 31 36 38 2e 31 2e  36 34 0d 0a 46 72 6f 6d   2.168.1. 64··From
00f0  3a 20 22 31 36 31 37 38  37 36 36 31 31 31 22 20   : "16178 766111"
0100  3c 73 69 70 3a 31 36 31  37 38 37 36 36 31 31 31   <sip:161 78766111
0110  40 74 2e 76 6f 6e 63 70  2e 63 6f 6d 3a 31 30 30   @t.voncp .com:100
0120  30 30 3e 3b 74 61 67 3d  36 63 35 36 66 65 66 64   00>;tag= 6c56fefd
0130  34 64 35 64 33 33 62 0d  0a 54 6f 3a 20 22 31 36   4d5d33b· ·To: "16
```

Figure 10

3) Click on "Telephony" > "VoIP Calls". (in figure 11)



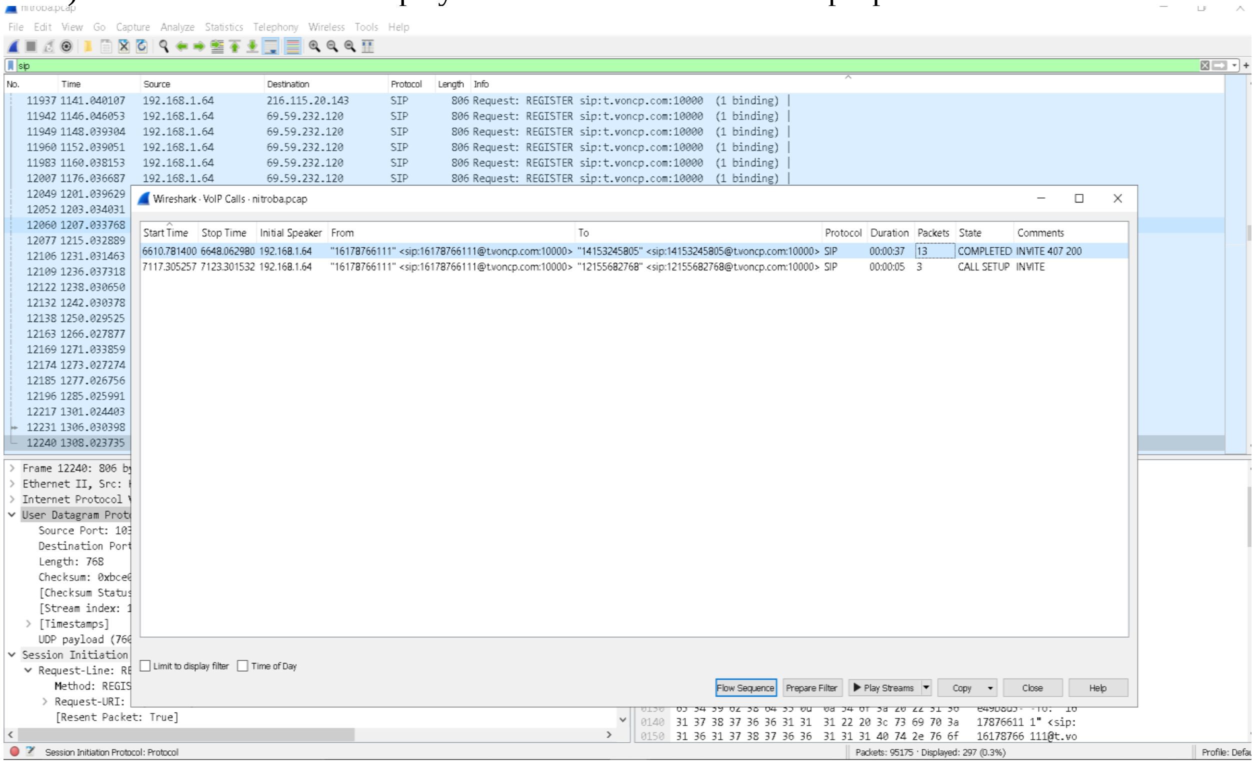
```
No.     Time          Source          ...                       otocol   Length  Info
  11937 1141.040107   192.168.1.64                              IP        806 Request: REGISTER sip:t.voncp.com
  11942 1146.046053   192.168.1.64                              IP        806 Request: REGISTER sip:t.voncp.com
  11949 1148.039304   192.168.1.64                              IP        806 Request: REGISTER sip:t.voncp.com
  11960 1152.039051   192.168.1.64                              IP        806 Request: REGISTER sip:t.voncp.com
  11983 1160.038153   192.168.1.64                              IP        806 Request: REGISTER sip:t.voncp.com
  12007 1176.036687   192.168.1.64                              IP        806 Request: REGISTER sip:t.voncp.com
  12049 1201.039629   192.168.1.64                              IP        806 Request: REGISTER sip:t.voncp.com
  12052 1203.034031   192.168.1.64                              IP        806 Request: REGISTER sip:t.voncp.com
  12060 1207.033768   192.168.1.64                              IP        806 Request: REGISTER sip:t.voncp.com
  12077 1215.032889   192.168.1.64                              IP        806 Request: REGISTER sip:t.voncp.com
  12106 1231.031463   192.168.1.64                              IP        806 Request: REGISTER sip:t.voncp.com
  12109 1236.037318   192.168.1.64                              IP        806 Request: REGISTER sip:t.voncp.com
  12122 1238.030650   192.168.1.64                              IP        806 Request: REGISTER sip:t.voncp.com
  12132 1242.030378   192.168.1.64                              IP        806 Request: REGISTER sip:t.voncp.com
  12138 1250.029525   192.168.1.64                              IP        806 Request: REGISTER sip:t.voncp.com
  12163 1266.027877   192.168.1.64                              IP        806 Request: REGISTER sip:t.voncp.com
  12169 1271.033859   192.168.1.64                              IP        806 Request: REGISTER sip:t.voncp.com
  12174 1273.027274   192.168.1.64    216.115.20.143            SIP       806 Request: REGISTER sip:t.voncp.com
  12185 1277.026756   192.168.1.64    216.115.20.143            SIP       806 Request: REGISTER sip:t.voncp.com
  12196 1285.025991   192.168.1.64    216.115.20.143            SIP       806 Request: REGISTER sip:t.voncp.com
  12217 1301.024403   192.168.1.64    216.115.20.143            SIP       806 Request: REGISTER sip:t.voncp.com
  12231 1306.030398   192.168.1.64    69.59.232.120             SIP       806 Request: REGISTER sip:t.voncp.com
  12240 1308.023735   192.168.1.64    69.59.232.120             SIP       806 Request: REGISTER sip:t.voncp.com

> Frame 12240: 806 bytes on wire (6448 bits), 806 bytes captured (6448 bits)
> Ethernet II, Src: HonHaiPr_2e:4f:61 (00:1d:d9:2e:4f:61), Dst: ARRISGro_99:98:68 (00:1d:6b:99:98:68)
> Internet Protocol Version 4, Src: 192.168.1.64, Dst: 69.59.232.120
v User Datagram Protocol, Src Port: 1035, Dst Port: 10000
      Source Port: 1035
      Destination Port: 10000
      Length: 768
      Checksum: 0xbce0 [unverified]
      [Checksum Status: Unverified]
      [Stream index: 140]
    > [Timestamps]
      UDP payload (760 bytes)
v Session Initiation Protocol (REGISTER)
    v Request-Line: REGISTER sip:t.voncp.com:10000 SIP/2.0
          Method: REGISTER
        > Request-URI: sip:t.voncp.com:10000
          [Resent Packet: True]

Session Initiation Protocol: Protocol
```

Figure 11

4) Wireshark will then display a list of all VoIP calls in the pcap file.


nitroba.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
sip
Wireshark · VoIP Calls · nitroba.pcap
□ Limit to display filter
□ Time of Day
Flow Sequence
Prepare Filter
▶ Play Streams
Copy
Close
Help

```
No.    Time          Source         Destination     Protocol  Length Info
 11937 1141.040107   192.168.1.64   216.115.20.143  SIP       806 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
 11942 1146.046053   192.168.1.64   69.59.232.120   SIP       806 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
 11949 1148.039304   192.168.1.64   69.59.232.120   SIP       806 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
 11960 1152.039051   192.168.1.64   69.59.232.120   SIP       806 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
 11983 1160.038153   192.168.1.64   69.59.232.120   SIP       806 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
 12007 1176.036687   192.168.1.64   69.59.232.120   SIP       806 Request: REGISTER sip:t.voncp.com:10000  (1 binding) |
```

Start Time	Stop Time	Initial Speaker	From	To	Protocol	Duration	Packets	State	Comments
6610.781400	6648.062980	192.168.1.64	"16178766111" <sip:16178766111@t.voncp.com:10000>	"14153245805" <sip:14153245805@t.voncp.com:10000>	SIP	00:00:37	13	COMPLETED	INVITE 407 200
7117.305257	7123.301532	192.168.1.64	"16178766111" <sip:16178766111@t.voncp.com:10000>	"12155682768" <sip:12155682768@t.voncp.com:10000>	SIP	00:00:05	3	CALL SETUP	INVITE

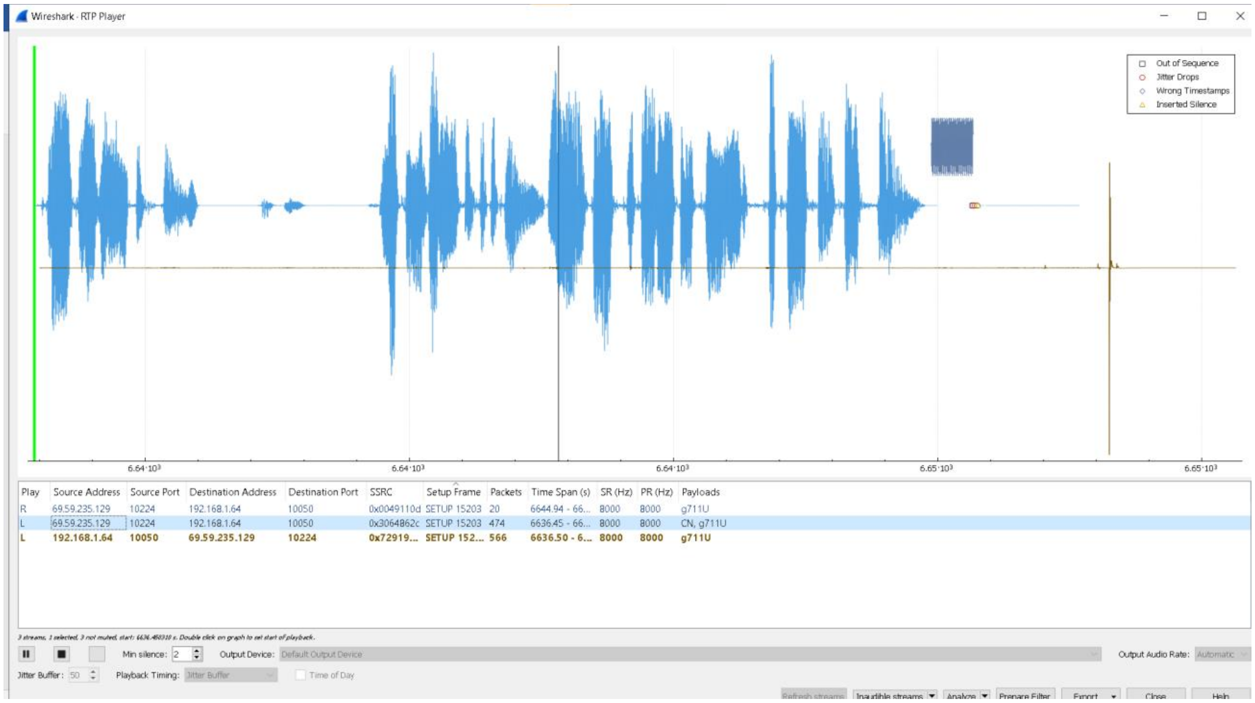
```
0140  31 37 38 37 36 36 31 31  31 22 20 3c 73 69 70 3a   17876611 1" <sip:
0150  31 36 31 37 38 37 36 36  31 31 31 40 74 2e 76 6f   16178766 111@t.vo

Session Initiation Protocol: Protocol      Packets: 95175 · Displayed: 297 (0.3%)      Profile: Defau
```

Figure 12

5) Select the VoIP call you want to extract and click on "Play Streams".

6) Wireshark will then extract the audio from the VoIP call and play it through your default media player or you can change it to a real-time player (RTP).



Play	Source Address	Source Port	Destination Address	Destination Port	SSRC	Setup Frame	Packets	Time Span (s)	SR (Hz)	PR (Hz)	Payloads
R	69.59.235.129	10224	192.168.1.64	10050	0x0049110d	SETUP 15203	20	6644.94 - 66...	8000	8000	g711U
L	69.59.235.129	10224	192.168.1.64	10050	0x3064862c	SETUP 15203	474	6636.45 - 66...	8000	8000	CN, g711U
L	**192.168.1.64**	**10050**	**69.59.235.129**	**10224**	**0x72919...**	**SETUP 152...**	**566**	**6636.50 - 6...**	**8000**	**8000**	**g711U**

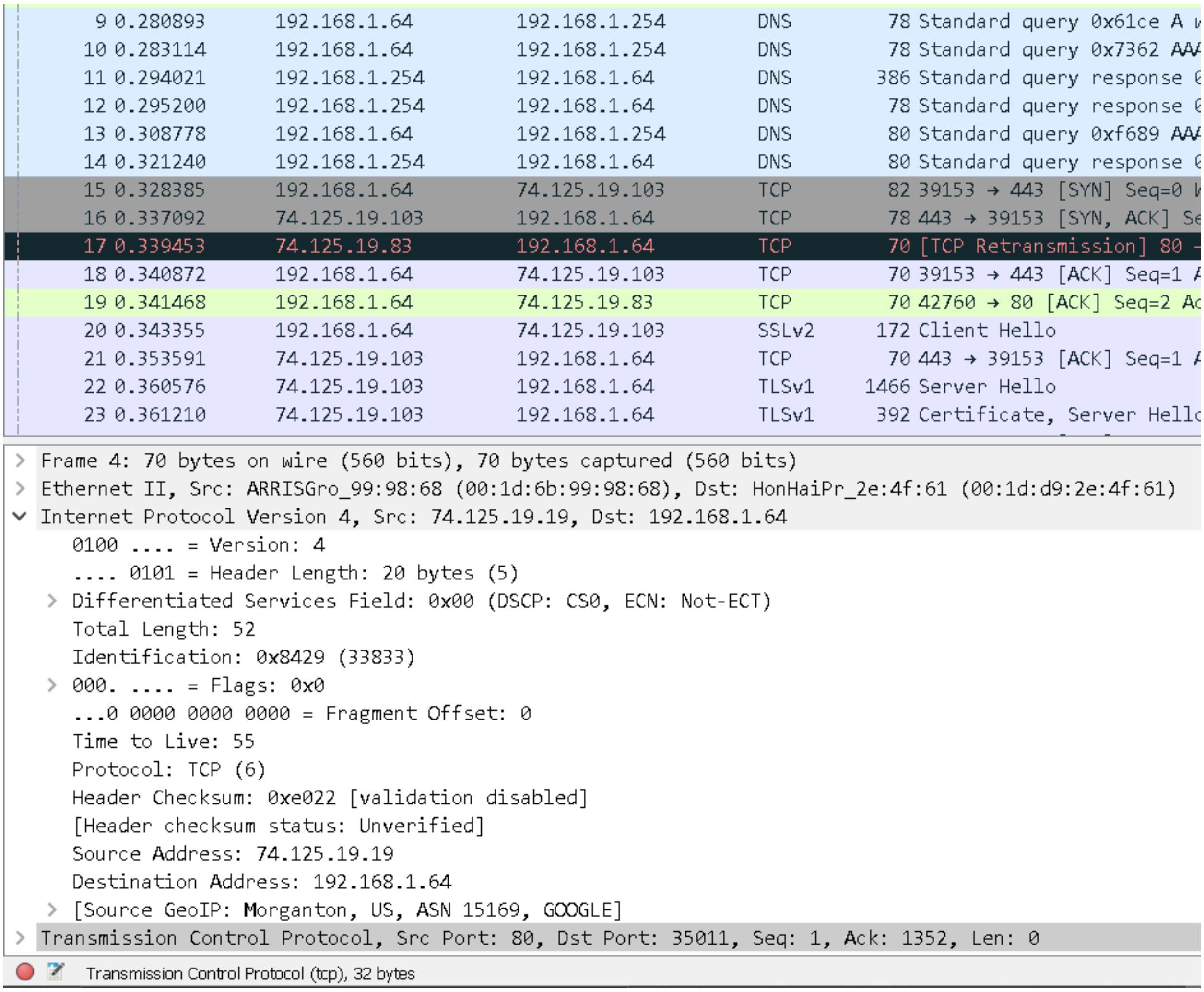
3 streams, 1 selected, 3 not muted, start: 6636.458310 s. Double click on graph to set start of playback.

Figure 13

GEOLOCATION OF THE IP ADDRESS:

1. install the GeoIP database from maxmind which contains the IP address of the system.
2. Open Wireshark and go to the "Edit" menu and select "Preferences".
3. In the Preferences dialog box, select "Name Resolution" from the list on the left.
4. Click the "Edit" button next to "GeoIP database directories".
5. Click the "New" button and select the folder where you saved the GeoIP database file.
6. Click the "OK" button to save the changes and close the dialog box.
7. Click the "OK" button in the Preferences dialog box to save the changes and close them.
8. 4) Restart Wireshark
9. A) Open the Pcap file you want to analysis
10. B) Statistics) Endpoints) IPv4) Map

NOW, we have geolocation for different Ip addresses.



```
  9 0.280893   192.168.1.64    192.168.1.254   DNS      78 Standard query 0x61ce A w
 10 0.283114   192.168.1.64    192.168.1.254   DNS      78 Standard query 0x7362 AAA
 11 0.294021   192.168.1.254   192.168.1.64    DNS     386 Standard query response 0
 12 0.295200   192.168.1.254   192.168.1.64    DNS      78 Standard query response 0
 13 0.308778   192.168.1.64    192.168.1.254   DNS      80 Standard query 0xf689 AAA
 14 0.321240   192.168.1.254   192.168.1.64    DNS      80 Standard query response 0
 15 0.328385   192.168.1.64    74.125.19.103   TCP      82 39153 → 443 [SYN] Seq=0 W
 16 0.337092   74.125.19.103   192.168.1.64    TCP      78 443 → 39153 [SYN, ACK] Se
 17 0.339453   74.125.19.83    192.168.1.64    TCP      70 [TCP Retransmission] 80 →
 18 0.340872   192.168.1.64    74.125.19.103   TCP      70 39153 → 443 [ACK] Seq=1 A
 19 0.341468   192.168.1.64    74.125.19.83    TCP      70 42760 → 80 [ACK] Seq=2 Ac
 20 0.343355   192.168.1.64    74.125.19.103   SSLv2   172 Client Hello
 21 0.353591   74.125.19.103   192.168.1.64    TCP      70 443 → 39153 [ACK] Seq=1 A
 22 0.360576   74.125.19.103   192.168.1.64    TLSv1  1466 Server Hello
 23 0.361210   74.125.19.103   192.168.1.64    TLSv1   392 Certificate, Server Hello
```

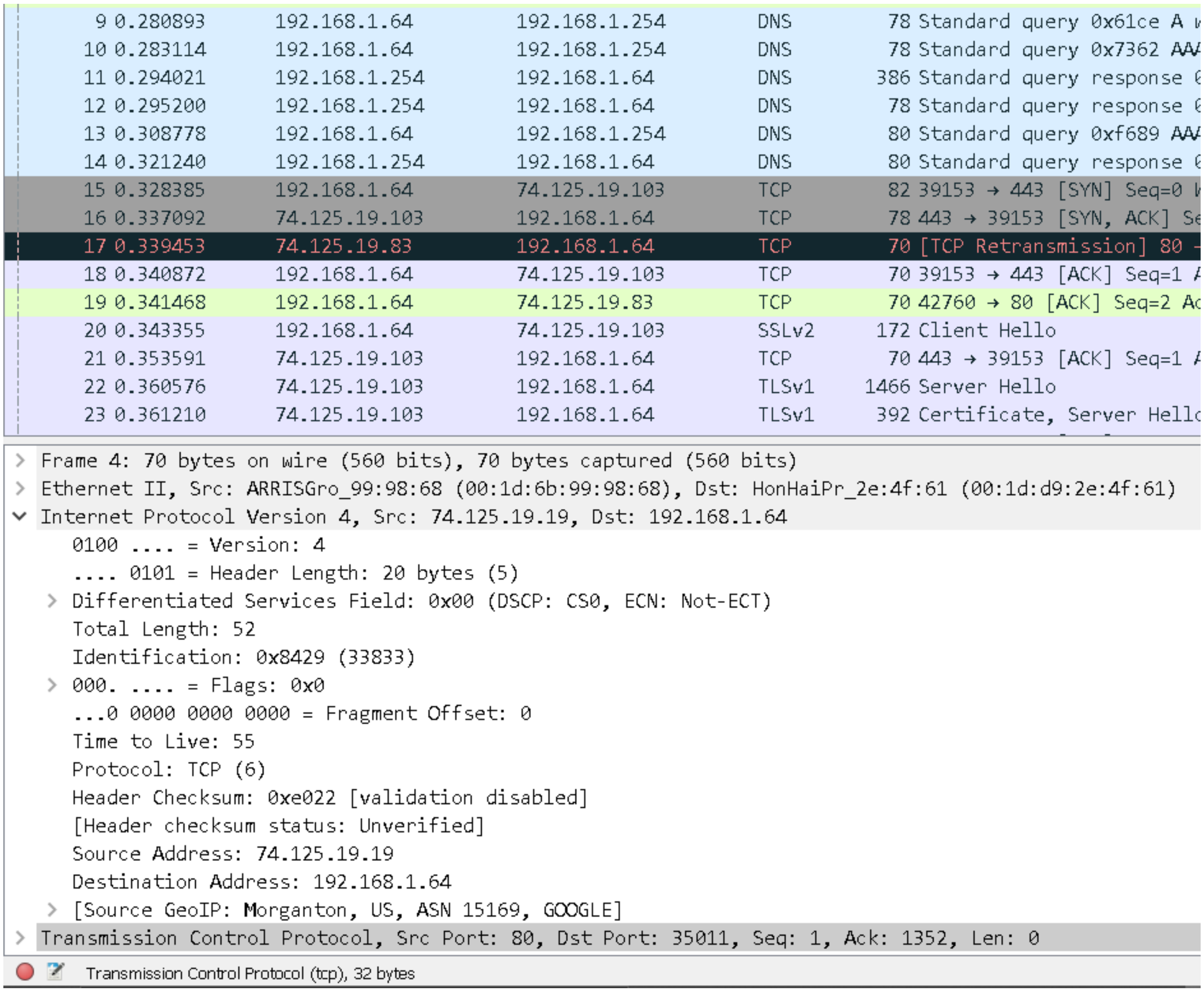
```
> Frame 4: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: ARRISGro_99:98:68 (00:1d:6b:99:98:68), Dst: HonHaiPr_2e:4f:61 (00:1d:d9:2e:4f:61)
v Internet Protocol Version 4, Src: 74.125.19.19, Dst: 192.168.1.64
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x8429 (33833)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 55
    Protocol: TCP (6)
    Header Checksum: 0xe022 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 74.125.19.19
    Destination Address: 192.168.1.64
  > [Source GeoIP: Morganton, US, ASN 15169, GOOGLE]
> Transmission Control Protocol, Src Port: 80, Dst Port: 35011, Seq: 1, Ack: 1352, Len: 0
```

Transmission Control Protocol (tcp), 32 bytes

Figure 14

.

The GeoIP tab will display the country, city, latitude, and longitude of the IP address.



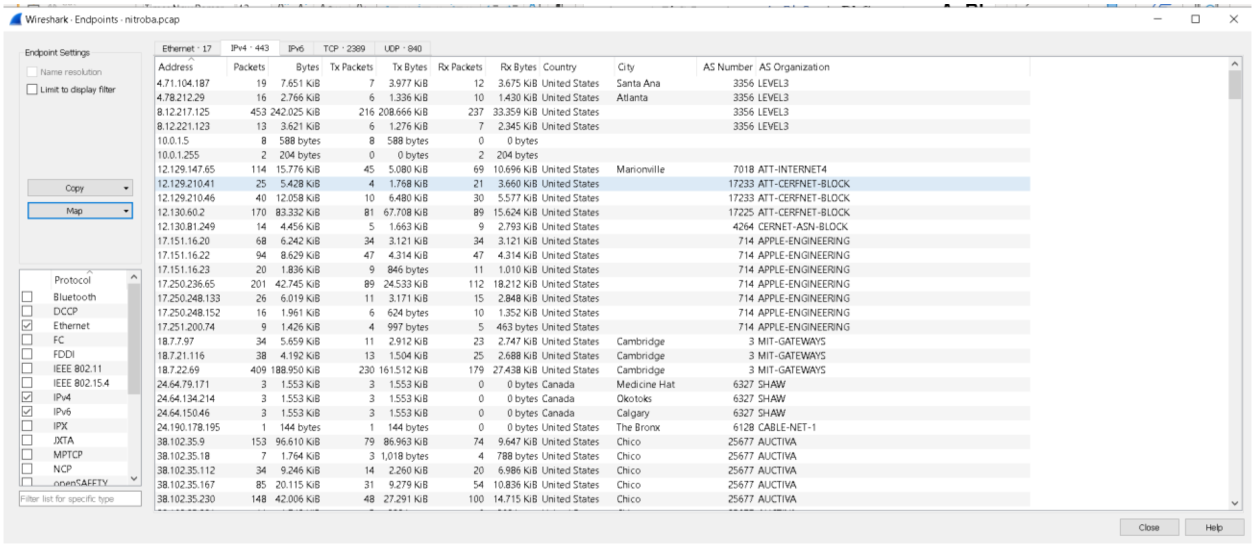
```
  9 0.280893   192.168.1.64    192.168.1.254   DNS      78 Standard query 0x61ce A w
 10 0.283114   192.168.1.64    192.168.1.254   DNS      78 Standard query 0x7362 AAA
 11 0.294021   192.168.1.254   192.168.1.64    DNS     386 Standard query response 0
 12 0.295200   192.168.1.254   192.168.1.64    DNS      78 Standard query response 0
 13 0.308778   192.168.1.64    192.168.1.254   DNS      80 Standard query 0xf689 AAA
 14 0.321240   192.168.1.254   192.168.1.64    DNS      80 Standard query response 0
 15 0.328385   192.168.1.64    74.125.19.103   TCP      82 39153 → 443 [SYN] Seq=0 W
 16 0.337092   74.125.19.103   192.168.1.64    TCP      78 443 → 39153 [SYN, ACK] Se
 17 0.339453   74.125.19.83    192.168.1.64    TCP      70 [TCP Retransmission] 80 →
 18 0.340872   192.168.1.64    74.125.19.103   TCP      70 39153 → 443 [ACK] Seq=1 A
 19 0.341468   192.168.1.64    74.125.19.83    TCP      70 42760 → 80 [ACK] Seq=2 Ac
 20 0.343355   192.168.1.64    74.125.19.103   SSLv2   172 Client Hello
 21 0.353591   74.125.19.103   192.168.1.64    TCP      70 443 → 39153 [ACK] Seq=1 A
 22 0.360576   74.125.19.103   192.168.1.64    TLSv1  1466 Server Hello
 23 0.361210   74.125.19.103   192.168.1.64    TLSv1   392 Certificate, Server Hello
```

```
> Frame 4: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
> Ethernet II, Src: ARRISGro_99:98:68 (00:1d:6b:99:98:68), Dst: HonHaiPr_2e:4f:61 (00:1d:d9:2e:4f:61)
v Internet Protocol Version 4, Src: 74.125.19.19, Dst: 192.168.1.64
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 52
    Identification: 0x8429 (33833)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 55
    Protocol: TCP (6)
    Header Checksum: 0xe022 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 74.125.19.19
    Destination Address: 192.168.1.64
  > [Source GeoIP: Morganton, US, ASN 15169, GOOGLE]
> Transmission Control Protocol, Src Port: 80, Dst Port: 35011, Seq: 1, Ack: 1352, Len: 0
```

Transmission Control Protocol (tcp), 32 bytes

Figure 15

Now we can see the end points of different Ip addresses



Endpoint Settings

□ Name resolution

□ Limit to display filter

	Protocol
□	Bluetooth
□	DCCP
☑	Ethernet
□	FC
□	FDDI
□	IEEE 802.11
□	IEEE 802.15.4
☑	IPv4
☑	IPv6
□	IPX
□	JXTA
□	MPTCP
□	NCP
□	openSAFETY

Filter list for specific type

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
4.71.104.187	19	7.651 KiB	7	3.977 KiB	12	3.675 KiB	United States	Santa Ana	3356	LEVEL3
4.78.212.29	16	2.766 KiB	6	1.336 KiB	10	1.430 KiB	United States	Atlanta	3356	LEVEL3
8.12.217.125	453	242.025 KiB	216	208.666 KiB	237	33.359 KiB	United States		3356	LEVEL3
8.12.221.123	13	3.621 KiB	6	1.276 KiB	7	2.345 KiB	United States		3356	LEVEL3
10.0.1.5	8	588 bytes	8	588 bytes	0	0 bytes				
10.0.1.255	2	204 bytes	0	0 bytes	2	204 bytes				
12.129.147.65	114	15.776 KiB	45	5.080 KiB	69	10.696 KiB	United States	Marionville	7018	ATT-INTERNET4
12.129.210.41	25	5.428 KiB	4	1.768 KiB	21	3.660 KiB	United States		17233	ATT-CERFNET-BLOCK
12.129.210.46	40	12.058 KiB	10	6.480 KiB	30	5.577 KiB	United States		17233	ATT-CERFNET-BLOCK
12.130.60.2	170	83.332 KiB	81	67.708 KiB	89	15.624 KiB	United States		17225	ATT-CERFNET-BLOCK
12.130.81.249	14	4.456 KiB	5	1.663 KiB	9	2.793 KiB	United States		4264	CERNET-ASN-BLOCK
17.151.16.20	68	6.242 KiB	34	3.121 KiB	34	3.121 KiB	United States		714	APPLE-ENGINEERING
17.151.16.22	94	8.629 KiB	47	4.314 KiB	47	4.314 KiB	United States		714	APPLE-ENGINEERING
17.151.16.23	20	1.836 KiB	9	846 bytes	11	1.010 KiB	United States		714	APPLE-ENGINEERING
17.250.236.65	201	42.745 KiB	89	24.533 KiB	112	18.212 KiB	United States		714	APPLE-ENGINEERING
17.250.248.133	26	6.019 KiB	11	3.171 KiB	15	2.848 KiB	United States		714	APPLE-ENGINEERING
17.250.248.152	16	1.961 KiB	6	624 bytes	10	1.352 KiB	United States		714	APPLE-ENGINEERING
17.251.200.74	9	1.426 KiB	4	997 bytes	5	463 bytes	United States		714	APPLE-ENGINEERING
18.7.7.97	34	5.659 KiB	11	2.912 KiB	23	2.747 KiB	United States	Cambridge	3	MIT-GATEWAYS
18.7.21.116	38	4.192 KiB	13	1.504 KiB	25	2.688 KiB	United States	Cambridge	3	MIT-GATEWAYS
18.7.22.69	409	188.950 KiB	230	161.512 KiB	179	27.438 KiB	United States	Cambridge	3	MIT-GATEWAYS
24.64.79.171	3	1.553 KiB	3	1.553 KiB	0	0 bytes	Canada	Medicine Hat	6327	SHAW
24.64.134.214	3	1.553 KiB	3	1.553 KiB	0	0 bytes	Canada	Okotoks	6327	SHAW
24.64.150.46	3	1.553 KiB	3	1.553 KiB	0	0 bytes	Canada	Calgary	6327	SHAW
24.190.178.195	1	144 bytes	1	144 bytes	0	0 bytes	United States	The Bronx	6128	CABLE-NET-1
38.102.35.9	153	96.610 KiB	79	86.963 KiB	74	9.647 KiB	United States	Chico	25677	AUCTIVA
38.102.35.18	7	1.764 KiB	3	1,018 bytes	4	788 bytes	United States	Chico	25677	AUCTIVA
38.102.35.112	34	9.246 KiB	14	2.260 KiB	20	6.986 KiB	United States	Chico	25677	AUCTIVA
38.102.35.167	85	20.115 KiB	31	9.279 KiB	54	10.836 KiB	United States	Chico	25677	AUCTIVA
38.102.35.230	148	42.006 KiB	48	27.291 KiB	100	14.715 KiB	United States	Chico	25677	AUCTIVA

Figure 16

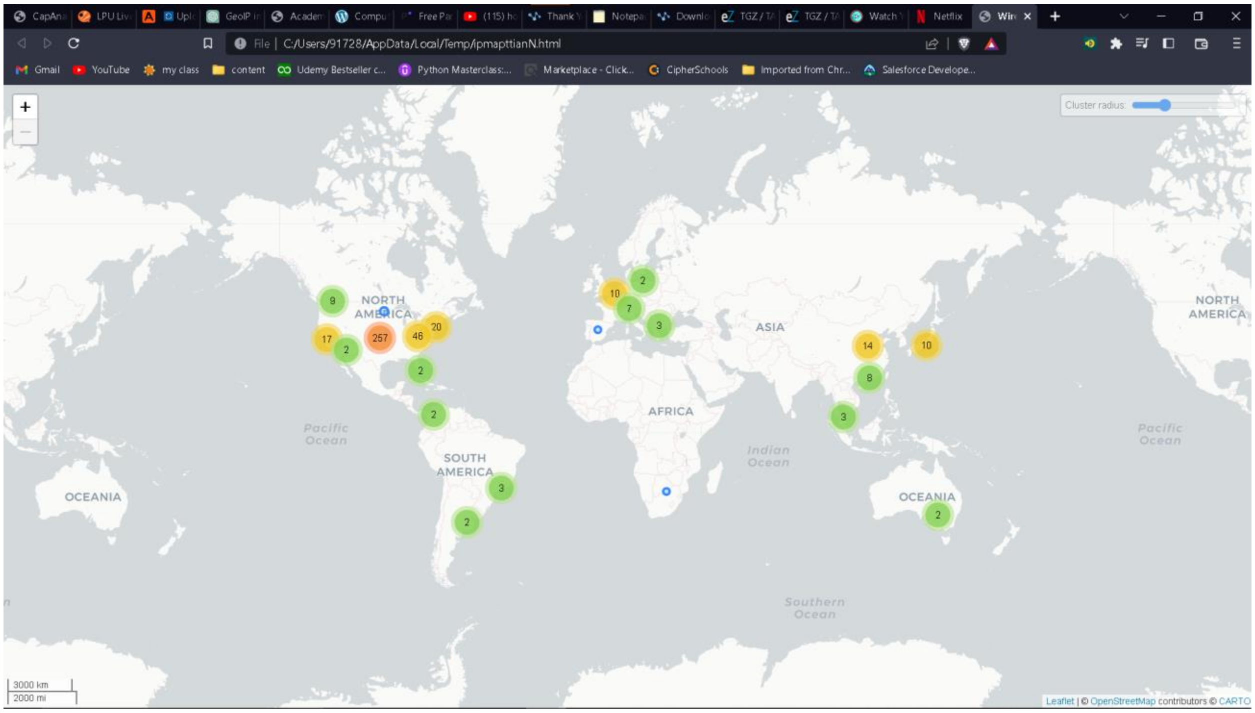


Figure 17

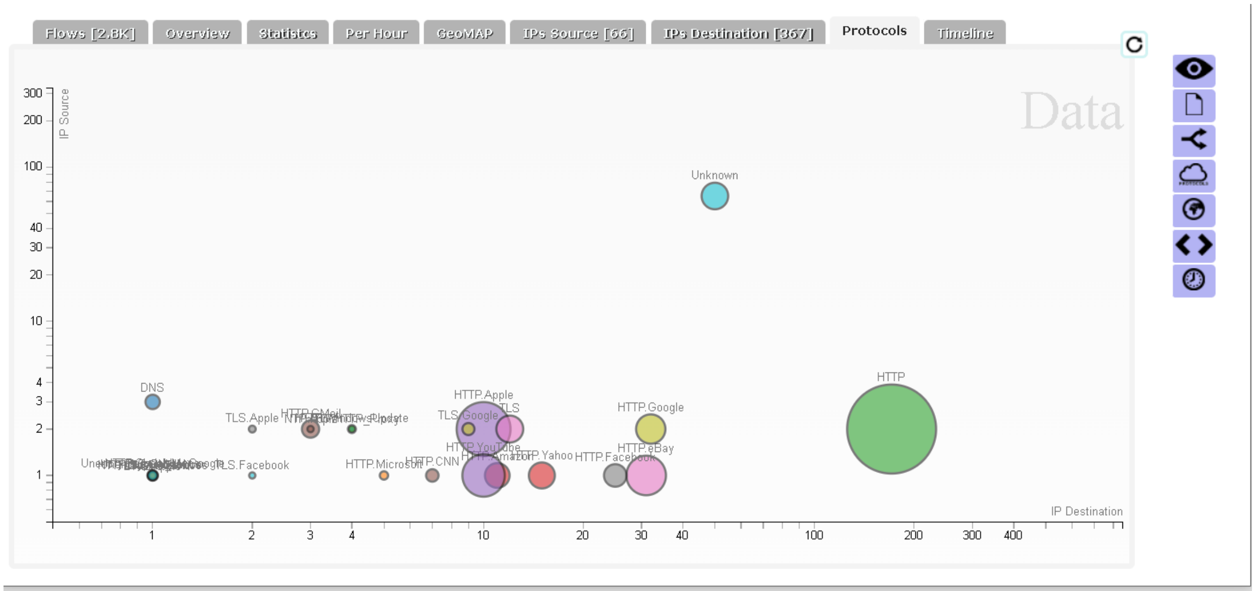


Figure 18

All the protocols that are in this .pcap file

In conclusion, Wireshark is a powerful network protocol analyzer that can capture and analyze network traffic for various applications. With the ability to capture and interpret data from various network protocols, Wireshark is an indispensable tool for network administrators and security professionals.

Using a pcap file as a reference, it is possible to extract various types of data from network traffic captured by Wireshark. With the help of open-source software such as Network Miner, it is possible to extract each email from POP, IMAP, and SMTP protocols, as well as all HTTP contents and each VoIP call.

Overall, the ability to extract and analyze data from network traffic can help identify and troubleshoot network issues, monitor network performance, and identify potential security threats. Wireshark remains a critical tool in the arsenal of any network professional, and its continued development and support ensure that it will remain an essential tool for years to come.

GITHUB LINK: https://github.com/Ganesh-007/INT-301