

PACKET CAPTURE ANALYSIS

Introduction

The dynamic evolution of technology has led to a complex interconnected world that forms networks in every aspect of our lives. We continue to depend on different technologies to automate or make our daily tasks easier. As the world of technology continues to bring different regions closer due to its flexibility it is vital to be aware of the rise in cybercriminals since this enlarges the attack surface in all possible angles. This paper focuses on a lab detailing the steps taken in network packet capture analysis using capturing tools to investigate data across a network. This interconnection creates a network where a packet is derived and can be defined as the smallest unit of data that is grouped and transferred over a network (An & Lu, 2016). This lab will be investigating a case of a suspect by the name “Ann” who is believed to have disappeared after being bailed out. We will be looking into a packet capture that is alleged to have her whereabouts.

Analysis

The suspect is believed to have visited online addresses which are shown and detailed below. The suspect at hand laptop address is Ann’s MAC address: 00:21:70: 4D:4F:AE which uniquely identifies the device in the captured network.

Cisco Inc

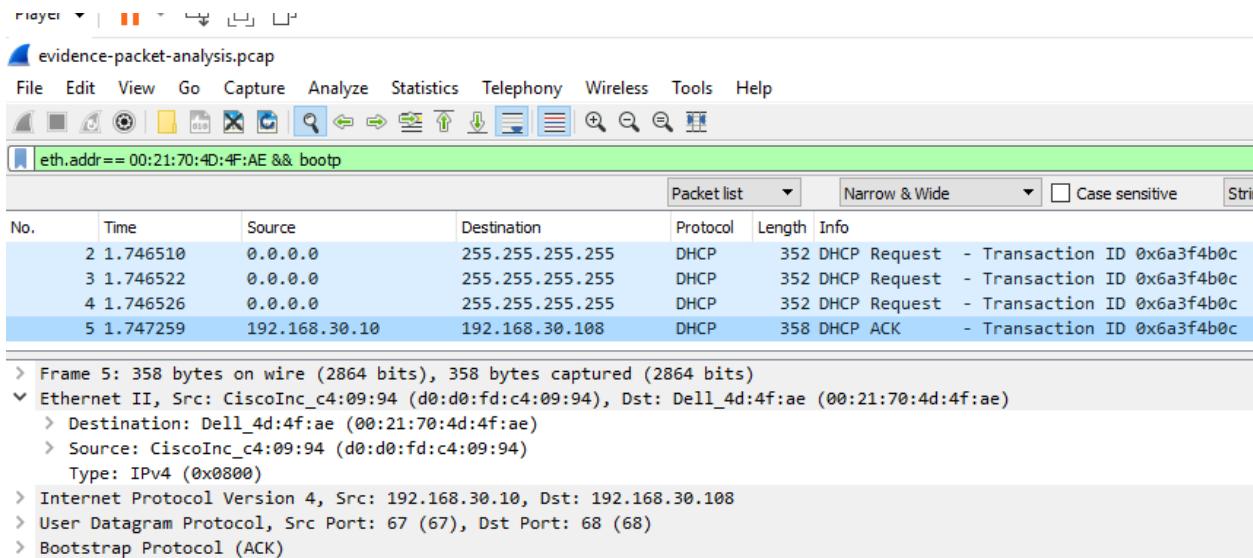


Figure 1/Cisco

The above screenshot shows that the laptop connects to a cisco device to access the network in the Internal network: 192.168.30.0/24. The list below shows the extended online addresses that the user visited.

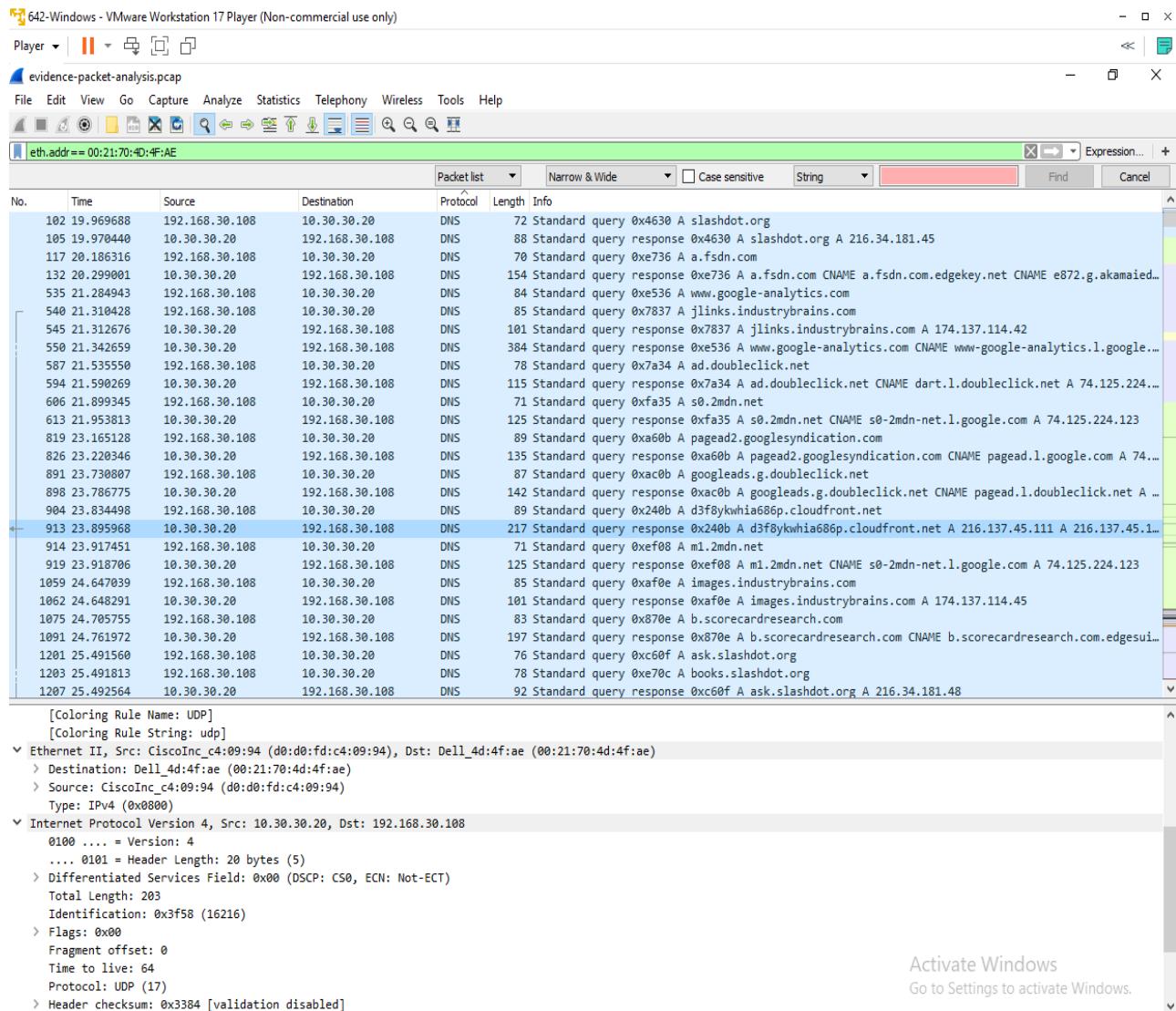


Figure 2/Addresses

The figure above shows some of the addresses visited such as slashdot.org , a.fsdn.com, jlinks.industrybrains.com et cetera. The above figure is grouped by the protocol DNS (Domain Name System) protocol that translates the ip addresses into domain names.

The credentials captured in the screenshots below are encoded with base64 and after decoding the results were:

```
c251YWt5ZzMza3k= -sneakyg33ky
czAwcGVyczNrcjF0 - s00pers3kr1t|
```

Figure 3/decoded

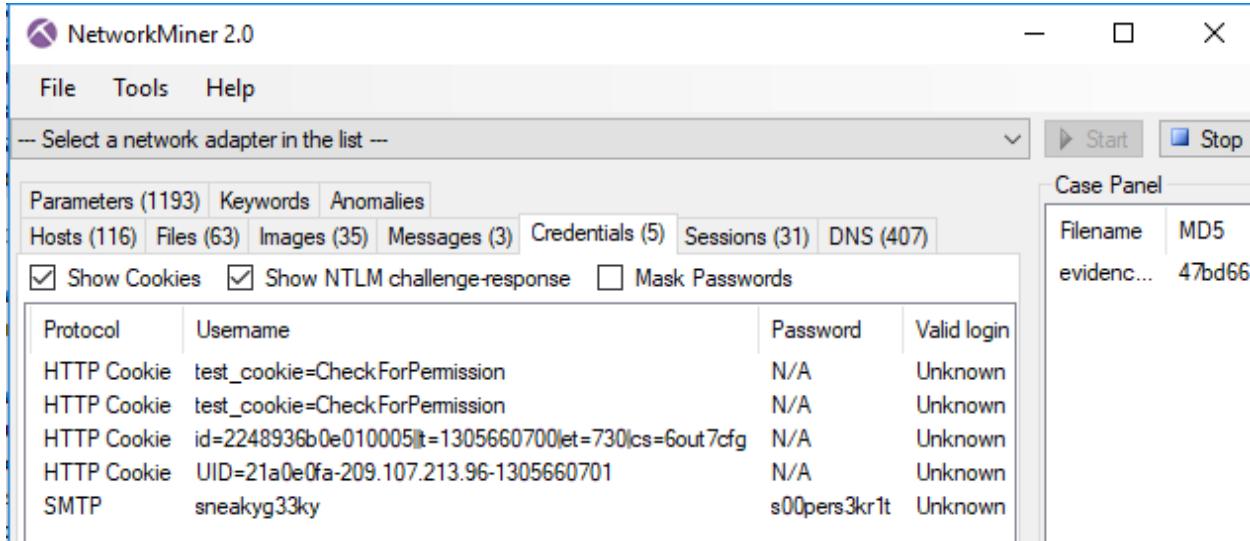


Figure 4/credentials

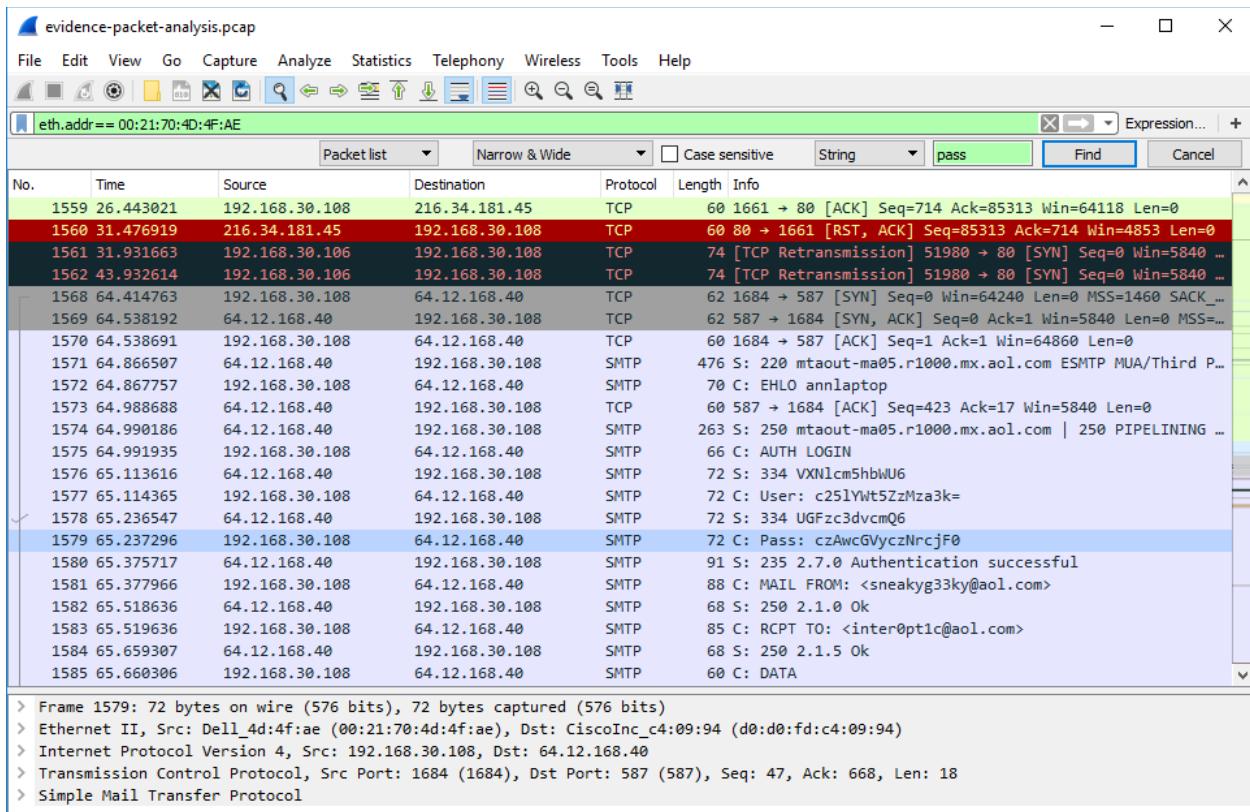
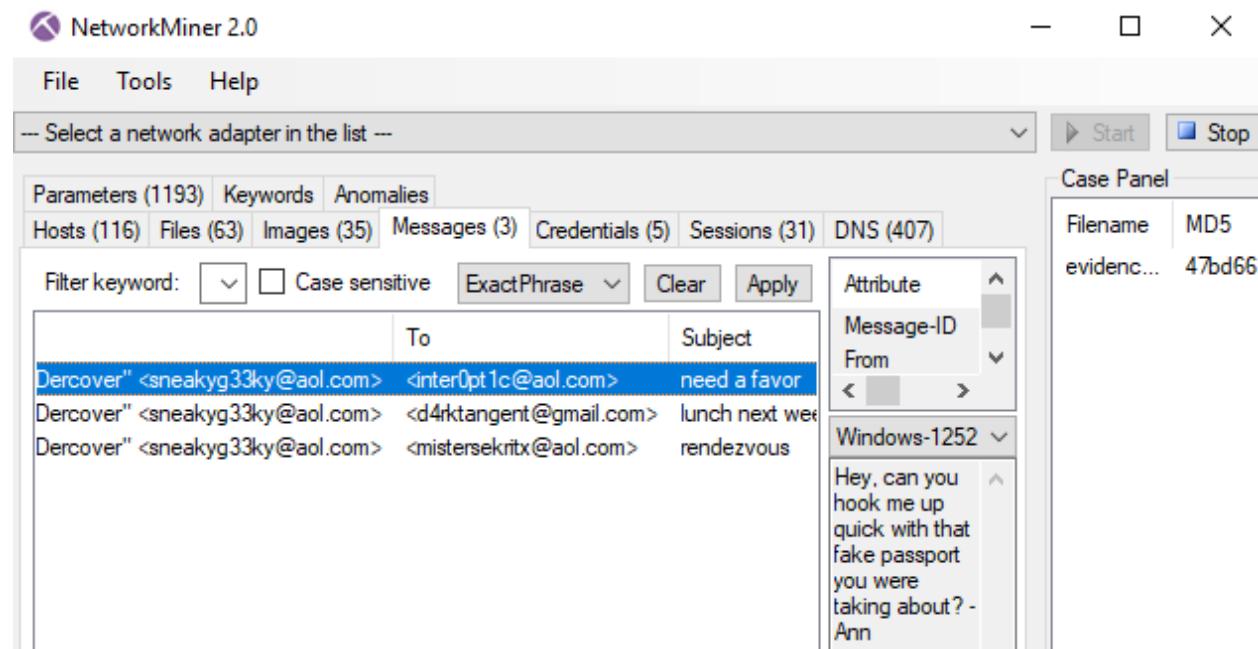


Figure 5/credentials

The above screenshot shows the web mail organization showing the credentials used for the login authorization.

The figures below show that Ann communicated with three other recipients with one alleged to be her lover. The emails are listed below.



The screenshot shows the NetworkMiner 2.0 interface. The main window displays a list of credentials, with the 'Credentials (5)' tab selected. The list shows three email entries:

	To	Subject	
Dercov...	<sneakyg33ky@aol.com>	<inter0pt1c@aol.com>	need a favor
Dercov...	<sneakyg33ky@aol.com>	<d4rktangent@gmail.com>	lunch next we...
Dercov...	<sneakyg33ky@aol.com>	<mistersekritx@aol.com>	rendezvous

On the right side, the 'Case Panel' shows the details of the selected email. The 'Attribute' section lists 'Message-ID' and 'From'. The 'Content' section shows the message body: "Hey, can you hook me up quick with that fake passport you were taking about? - Ann". The 'Windows-1252' encoding is selected.

evidence-packet-analysis.pcap						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
eth.addr== 00:21:70:4D:4F:AE						
No.	Time	Source	Destination	Protocol	Length	Info
1819	195.128970	192.168.30.108	64.12.168.40	SMTP	88	C: MAIL FROM: <sneakyg33ky@aol.com>
1579	65.237296	192.168.30.108	64.12.168.40	SMTP	72	C: Pass: czAwcGVyczNrcjF0
1741	134.516303	192.168.30.108	64.12.168.40	SMTP	72	C: Pass: czAwcGVyczNrcjF0
1817	194.980303	192.168.30.108	64.12.168.40	SMTP	72	C: Pass: czAwcGVyczNrcjF0
1593	66.183010	192.168.30.108	64.12.168.40	SMTP	60	C: QUIT
1755	135.536725	192.168.30.108	64.12.168.40	SMTP	60	C: QUIT
2140	201.597305	192.168.30.108	64.12.168.40	SMTP	60	C: QUIT
1745	134.803640	192.168.30.108	64.12.168.40	SMTP	88	C: RCPT TO: <d4rktangent@gmail.com>
1583	65.519636	192.168.30.108	64.12.168.40	SMTP	85	C: RCPT TO: <inter0pt1c@aol.com>
1821	195.267141	192.168.30.108	64.12.168.40	SMTP	88	C: RCPT TO: <mistersekritx@aol.com>
1577	65.114365	192.168.30.108	64.12.168.40	SMTP	72	C: User: c25lYwt5ZzMza3k=
1739	134.390125	192.168.30.108	64.12.168.40	SMTP	72	C: User: c25lYwt5ZzMza3k=
1815	194.850627	192.168.30.108	64.12.168.40	SMTP	72	C: User: c25lYwt5ZzMza3k=
5	1.747259	192.168.30.10	192.168.30.108	DHCP	358	DHCP ACK - Transaction ID 0x6a3f4b0c
2	1.746510	0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0x6a3f4b0c
3	1.746522	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0x6a3f4b0c
4	1.746526	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0x6a3f4b0c
111	20.074129	192.168.30.108	216.34.181.45	HTTP	420	GET / HTTP/1.1
928	24.004152	192.168.30.108	74.125.224.123	HTTP	440	GET /1251053/1x1white.gif HTTP/1.1
941	24.090354	192.168.30.108	216.137.45.111	HTTP	479	GET /1live/leadgen/SD_RelatedResources_Top.gif HTTP/1.1
943	24.108843	192.168.30.108	216.137.45.111	HTTP	475	GET /1live/leadgen/SD_wrapper7b_bottom.png HTTP/1.1
620	22.128965	192.168.30.108	74.125.224.123	HTTP	455	GET /3000209/728x90_Endframe_Revised.jpg HTTP/1.1

Figure 6/Emails

The contents of the email conversations above were captured below, detailing what Ann was up to and what she was trying to do. The mail aol is a free mail that offers features like spam blocking, news, security ,weather et cetera which was used by Ann to do her communication (Aol, n.d.).

```

> From: "Ann Dercover" <sneakyg33ky@aol.com>, 1 item
> To: <d4rktangent@gmail.com>, 1 item
  Subject: lunch next week
  Date: Tue, 17 May 2011 13:33:26 -0600

<DIV><FONT face=3DArial size=3D2>Sorry-- I can't do lunch next week =\r\n
after all.=20\r\n
Heading out of town. Another time!</FONT></DIV>\r\n

Message-ID: <00ab01cc14c9$227de600$6b1ea8c0@annlaptop>
From: "Ann Dercover" <sneakyg33ky@aol.com>, 1 item
To: <inter0pt1c@aol.com>, 1 item
  Subject: need a favor
  Date: Tue, 17 May 2011 13:32:17 -0600

```

```
<DIV><FONT face=3DArial size=3D2>Hey, can you hook me up quick with that =\r\n
fake=20\r\n
passport you were taking about? - Ann</FONT></DIV>\r\n
```

Message-ID: <00bc01cc14c9\$6fd1bc60\$6b1ea8c0@annlaptop>
 From: "Ann Dercov" <sneakyg33ky@aol.com>, 1 item
 To: <mistersekritx@aol.com>, 1 item
 Subject: rendezvous
 Date: Tue, 17 May 2011 13:34:26 -0600

▼ Line-based text data: text/plain

Hi sweetheart! Bring your fake passport and a bathing suit. Address =\r\n
 attached. love, Ann

Figure 7/Transcripts

Ann had a conversation with a recipient allegedly her lover and they did share files where she was given the address to where they were to meet up which indicates a clue of her physical whereabouts. The figure below shows the google maps details of the physical address.

Meet me at the fountain near the rendezvous point. Address below. I'm bringing all the cash.

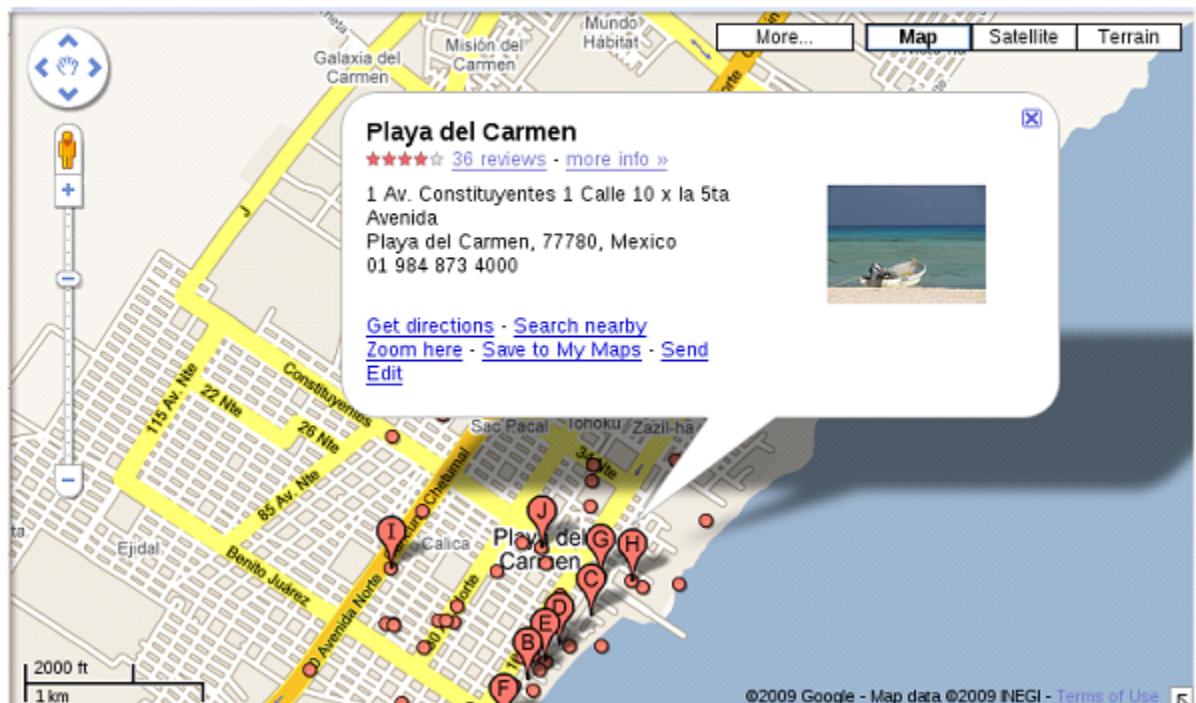


Figure 8/Location

Glossary

Domain Name system (DNS) – This is a system that is used to translate human friendly hostname into ip addresses (P.Hoffman & K.Fujiwara, 2024).
 Mac addresses – this a unique identifier assigned to a network interface controller for use as a network address in communication (Celestin & Mathieu, 2016).

References

- An, X., & Lu, X. (2016). Packet Capture and Protocol Analysis Based on Winpcap. *2016 International Conference on Robots & Intelligent System (ICRIS)*, 272-275.
- Aol.* (n.d.). Retrieved from
https://login.aol.com/?src=mail&client_id=dj0yJmk9VIN3cDhpNm1Id0szJmQ9WVdrOVdtRm1aMVU1Tm1zbWNHbzlNQS0tJnM9Y29uc3VtZXJzZWNyZXQmeD1mYQ--&crumb=pPgrPaOJNvs&lang=en-US&redirect_uri=https%3A%2F%2Foidc.mail.aol.com%2Fcallback&pspid=972825001&activity=mail-direc
- Celestin, M., & Mathieu, C. (2016). Defeating MAC Address Randomization Through Timing Attacks. *WiSec: Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, 15-20.
- P.Hoffman, & K.Fujiwara. (2024). Best Current Practice. *Internet Engineering Task Force*.

