SEPTEMBER 15, 2024

EVENT ANALYSIS

LAB 01

ANTHONY CAMPBELL YVW316

Professor McCulley

University of Texas at San Antonio IS 3523

Contents

Introduction

This lab focuses on the analysis of captured network traffic using a variety of security tools such as Wireshark, Network Miner, and SNORT via the SimSpace Cyber Range. We will examine the captured traffic to determine if any suspicious or malicious activity occurred, and through detailed analysis of the packet data or triggered alerts uncover the identity of any potential security threats.

Analysis

Though I have some experience with both Network Miner and Wireshark, I have more experience and therefore more familiar with the latter. So, after logging into SimSpace kali-hunt and win-hunt VMs, I find the Lab1PCAP file and open it up in Wireshark and NetworkMiner to begin. I would later try to use whatismyip.com's IP lookup tool, but the difference of twenty years makes this difficult to be accurate. SNORT was also useful in confirming suspicions draw from

Capture Length, Number, and Bytes

To find this information is simple, I go to the "Statistics" menu at the top and select "Capture File Properties" to see the frame details of the very first and last frames, as well as the elapsed time. Timestamped Oct 30, 2005 16:29:35 and Oct 30, 2005 16:38:00 respectively, the session capture lasted 8 minutes and 25 seconds. (see Appendix 1: Capture File Properties)

In this same Capture File Properties window, we can also see the number of packets, which is a total of 2449 packets. We are also able to see how many bytes were captured, which is a total of 811,157. (see Appendix 1: Capture File Properties)

The captured data appears to be a moderate level of activity on the network, potentially just routine traffic such as browsing, background processes, and small file transfers as opposed to large data transfers as that would involve a much larger number of bytes. The packet size distribution, and protocol types observed will provide further insight into the purpose of the captured traffic. (see Appendix 5: Packets / Bytes Breakdown)

Protocols Observed and Bulk of Transmission

Opening the “Protocol Hierarchy Statistics” window, under Statistics, we can see the entire breakdown of protocols observed. The affected party has stated that they only use the network for internet access to read mail, and the initial impression is that, with 84.9% of the packets being Transmission Control Protocol, for a home network mostly used to read email this seems typical. (seeAppendix 2: Protocol Hierarchy)

Within the “IO Graphs” of Wireshark we can see exactly when the bulk of data is transmitted and while there are a few spikes of data transmission the largest spike begins about the 94 second mark, and ends around the 96 second mark. A quick investigation reveals that these packets are HTTP and TCP that are accessing image files. (see Appendix 3: I/O Graph)

Service Providers , Host Computer Information, Credentials

During the capture an ISP was accessed, “homeportal.gateway.2wire.net” and was assigned the IP 172.16.0.1. The host machine had the name of “KaufmanUpstairs” and “KAUFMANUPSTAIRS<00>.” The IP address for the host is 172.16.1.35. While looking over and confirming device host, I notice and first become suspicious of a second “KaufmanUpstairs” device with a different IP address, but same MAC address – whatever this device is it is using the same communication hardware as the affected party’s home device, now officially highly suspected to be an affected device now. The operating system for the *real* Kaufman upstairs device is Windows 2000. (see Appendix 4: Affected Device and Router information, Appendix 6: IP Network Camera)

Using NetworkMiner we can see 11 servers had used some form of credentials. All but one utilizes HTTP Cookie protocol, the last using TCP which would cause me to look further into the server and its related IP address, its communications, in Wireshark. Other than that outlier the other servers are all mail related servers that sound like the typical use the affected party described. (see Appendix 7: Credentials Captured)

Local Network, Devices, and Access

A few other devices are on the local network. We have the following devices, and corresponding IP.

homeportal.gateway.2wire.net – 172.16.0.1, the WAN connection device

KaufmanUpstairs – 172.16.1.35, affected device and home computer

DVR-8525.local – 172.16.1.37, a DVR device which was very popular at home at the time.

“KaufmanUpstairs” – 172.16.1.39, the IP network camera

While it does not appear that much interaction between other devices on the network initially, there are several broadcasts that do reach other devices as the source of NBNS as well as some TiVoConnect packets are between host 172.16.1.35 and 172.16.255.255 so while they may not communicate directly, the broadcast is reaching all devices on the local network.

The Other Device

The previously mentioned “KaufmanUpstairs” is what would be considered ‘other’ as it does not belong on the affected party’s network. There are 10 packets associated with this device but they are quite telling. (see Appendix 12: 172.16.1.39 Packets)

The Story

The captured network data ultimately shows that the device has been compromised. The affected user has become the victim of a Man in the Middle attack, with evidence of ARP poisoning and/or Broadcast Name Resolution poisoning present. A bad actor is using the “IP Camera Device” to perform this, in packets no. 37 and 43 the MAC address associated with the device is 00:0f:66:15:06:14 amidst a great number of ARP requests before spoofing the MAC address of KaufmanUpstairs (which it conveniently shares the same device name with) of 00:40:ca:70:19:a3. (see Appendix 14: Prior MAC amidst ARP Flood)

Because there is an incredible volume of ARP packets, ARP poisoning is my suspicion as devices making requests often or unprompted can are a good indication of it occurring as user “sourabhsahu22” [1] provides in an article. For further comparison, I ran a much larger capture on my own device and noted that the ARP volume in Kaufman’s capture was much larger. (see Appendix 13: Gratuitous ARP packets)

From there I get out of my depth, but I am initially suspicious of communications after the spoofing between the Kaufman home device and a server, IP 66.39.22.157, as Kaufman stated that the use of the device is specifically email however a connection is made to transfer multiple files starting from packet 63. If we look at packet 73 we see request and response for user credentials. It could be that this was just forgotten and not mentioned, as checking in a separate virtualized environment shows that the website it mentions in info is some sort of Security website, but also in this exercise they may be playing the role of a bad actor offloading files. The connection is established again around packet 1524. In NetworkMiner I also find in the anomalies tab a second confirmation that ARP spoofing is in play. (see Appendix 11: NetworkMiner ARP Spoofing)

Snort

I am unsure if someone accidentally sabotaged SNORT on the machine I was on, but thankfully the SNORT documentation [2] is very helpful in providing the basics and I also used snort –help within the terminal as well. It detected many alerts that makes me believe that the bad actor may be using the host device to seek other vulnerable parties. (see Appendix 8: Snort Other HTTP Server, Appendix 9: Snort TCP Portsweep, Appendix 10: Snort TCP Small Segment Threshold) With the unknown traffic and data leak alerts flagged, I feel fairly confident that the device is compromised.

Conclusion

Based on the analysis of the captured network traffic, there is strong evidence that the affected user’s network has been compromised. The presence of multiple ARP requests, the use of identical MAC address for different devices, and ARP poisoning alerts indicate that a Man-in-the-Middle attack occurred. The “KaufmanUpstairs” IP Network Camera device with the same MAC address as the host computer of the same name appears to be the primary tool used by the attacker to spoof legitimate communications, masking its malicious actions as ordinary network traffic.

While the exact nature of the attack is beyond the scope of my current skill level, the evidence I gathered from Wireshark, NetworkMiner, and SNORT confirms that malicious activity took place. The affected party should (or hopefully in 2005 did) take immediate steps to mitigate the damage including resetting devices, updating firmware, and implementing stronger security measures to prevent future attacks that are similar.

References

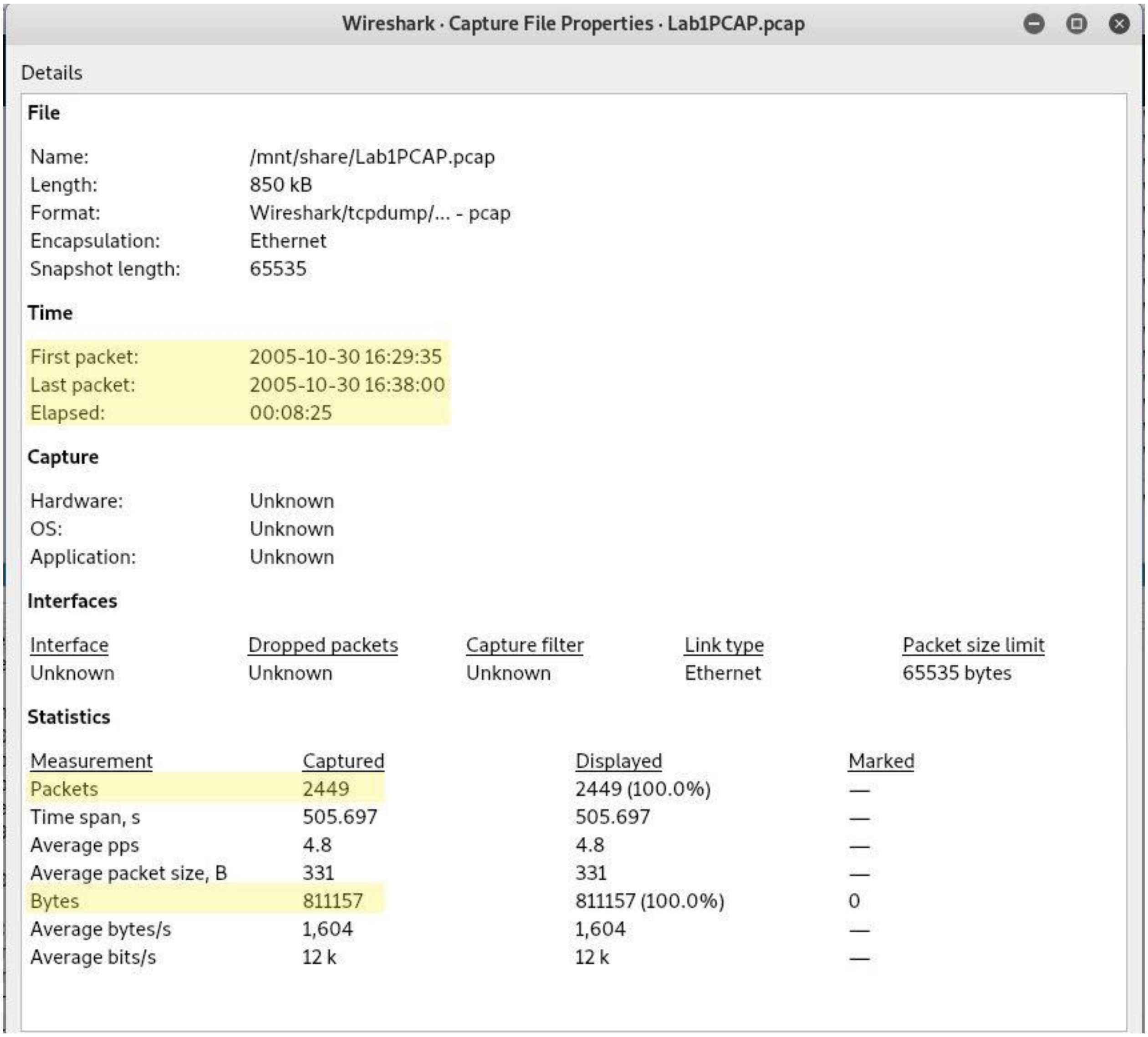
[1] "sourabhsahu22", "wireshark sniffing and spoofing," geeksforgeeks, 29 Jan 2024. [Online]. Available: https://www.geeksforgeeks.org/wireshark-sniffing-and-spoofing/. [Accessed 13 Sept 2024].

[2] SNORT, "Command Line Basics," SNORT, n.d. n.d. n.d.. [Online]. Available: https://docs.snort.org/start/help. [Accessed 14 Sept 2024].

[3] UTSA ISCS 3523 Event Analysis, "Lab01 Event Analysis," UTSA, n.d. n.d. n.d.. [Online]. Available: https://utsa.instructure.com/courses/47665/files/6962841?wrap=1. [Accessed 10 Sept 2024].

Appendices

Appendix 1: Capture File Properties



Wireshark · Capture File Properties · Lab1PCAP.pcap

Details

File

Name:	/mnt/share/Lab1PCAP.pcap
Length:	850 kB
Format:	Wireshark/tcpdump/... - pcap
Encapsulation:	Ethernet
Snapshot length:	65535

Time

First packet:	2005-10-30 16:29:35
Last packet:	2005-10-30 16:38:00
Elapsed:	00:08:25

Capture

Hardware:	Unknown
OS:	Unknown
Application:	Unknown

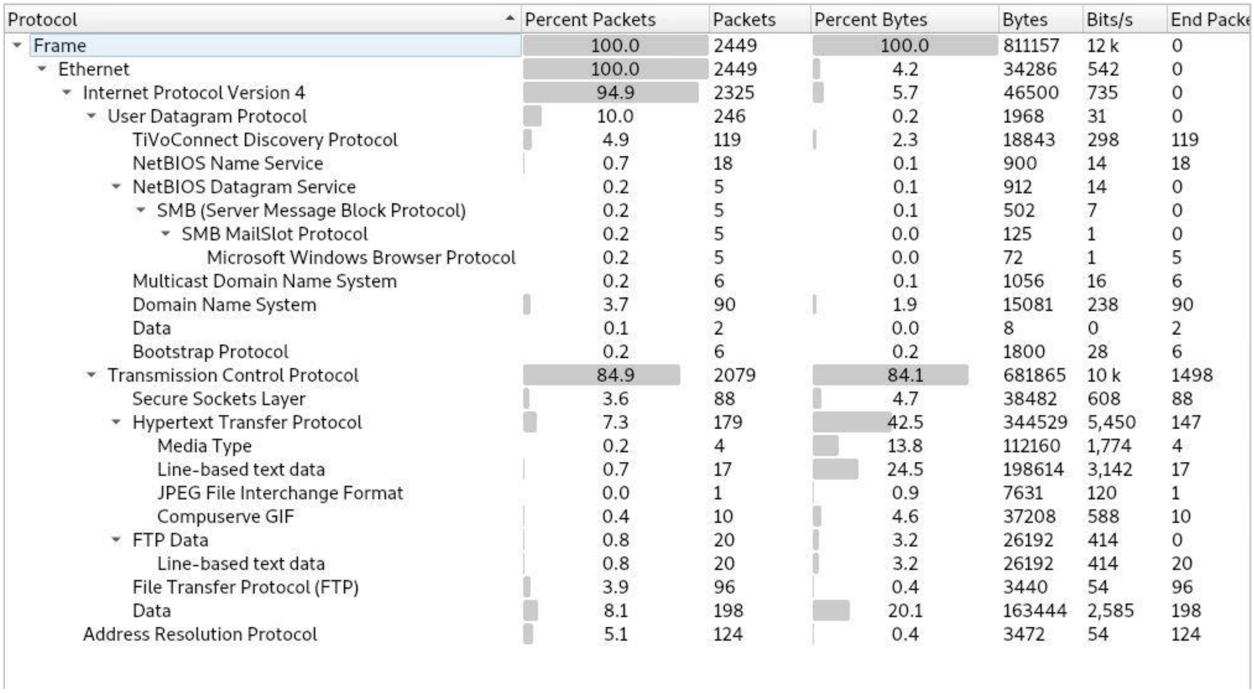
Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit
Unknown	Unknown	Unknown	Ethernet	65535 bytes

Statistics

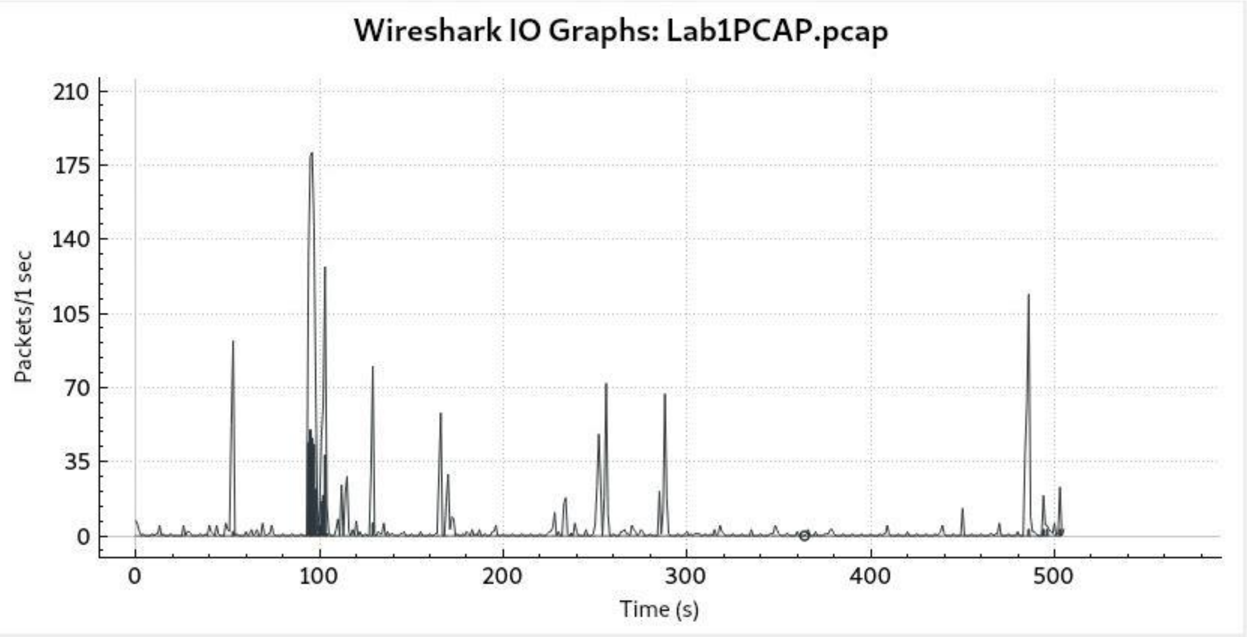
Measurement	Captured	Displayed	Marked
Packets	2449	2449 (100.0%)	—
Time span, s	505.697	505.697	—
Average pps	4.8	4.8	—
Average packet size, B	331	331	—
Bytes	811157	811157 (100.0%)	0
Average bytes/s	1,604	1,604	—
Average bits/s	12 k	12 k	—

Appendix 2: Protocol Hierarchy

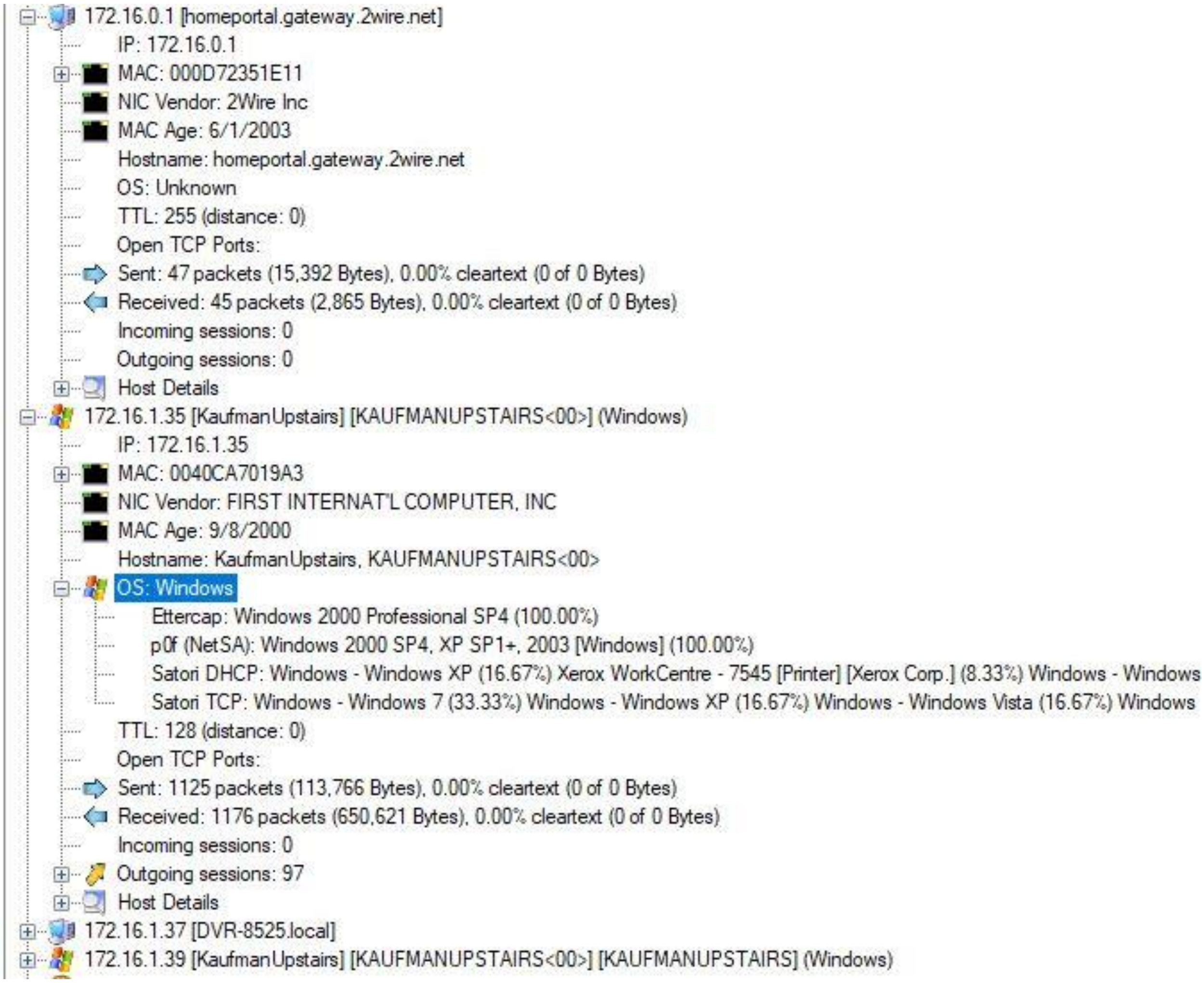


Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packe
Frame	100.0	2449	100.0	811157	12 k	0
Ethernet	100.0	2449	4.2	34286	542	0
Internet Protocol Version 4	94.9	2325	5.7	46500	735	0
User Datagram Protocol	10.0	246	0.2	1968	31	0
TiVoConnect Discovery Protocol	4.9	119	2.3	18843	298	119
NetBIOS Name Service	0.7	18	0.1	900	14	18
NetBIOS Datagram Service	0.2	5	0.1	912	14	0
SMB (Server Message Block Protocol)	0.2	5	0.1	502	7	0
SMB MailSlot Protocol	0.2	5	0.0	125	1	0
Microsoft Windows Browser Protocol	0.2	5	0.0	72	1	5
Multicast Domain Name System	0.2	6	0.1	1056	16	6
Domain Name System	3.7	90	1.9	15081	238	90
Data	0.1	2	0.0	8	0	2
Bootstrap Protocol	0.2	6	0.2	1800	28	6
Transmission Control Protocol	84.9	2079	84.1	681865	10 k	1498
Secure Sockets Layer	3.6	88	4.7	38482	608	88
Hypertext Transfer Protocol	7.3	179	42.5	344529	5,450	147
Media Type	0.2	4	13.8	112160	1,774	4
Line-based text data	0.7	17	24.5	198614	3,142	17
JPEG File Interchange Format	0.0	1	0.9	7631	120	1
Compuserve GIF	0.4	10	4.6	37208	588	10
FTP Data	0.8	20	3.2	26192	414	0
Line-based text data	0.8	20	3.2	26192	414	20
File Transfer Protocol (FTP)	3.9	96	0.4	3440	54	96
Data	8.1	198	20.1	163444	2,585	198
Address Resolution Protocol	5.1	124	0.4	3472	54	124

Appendix 3: I/O Graph

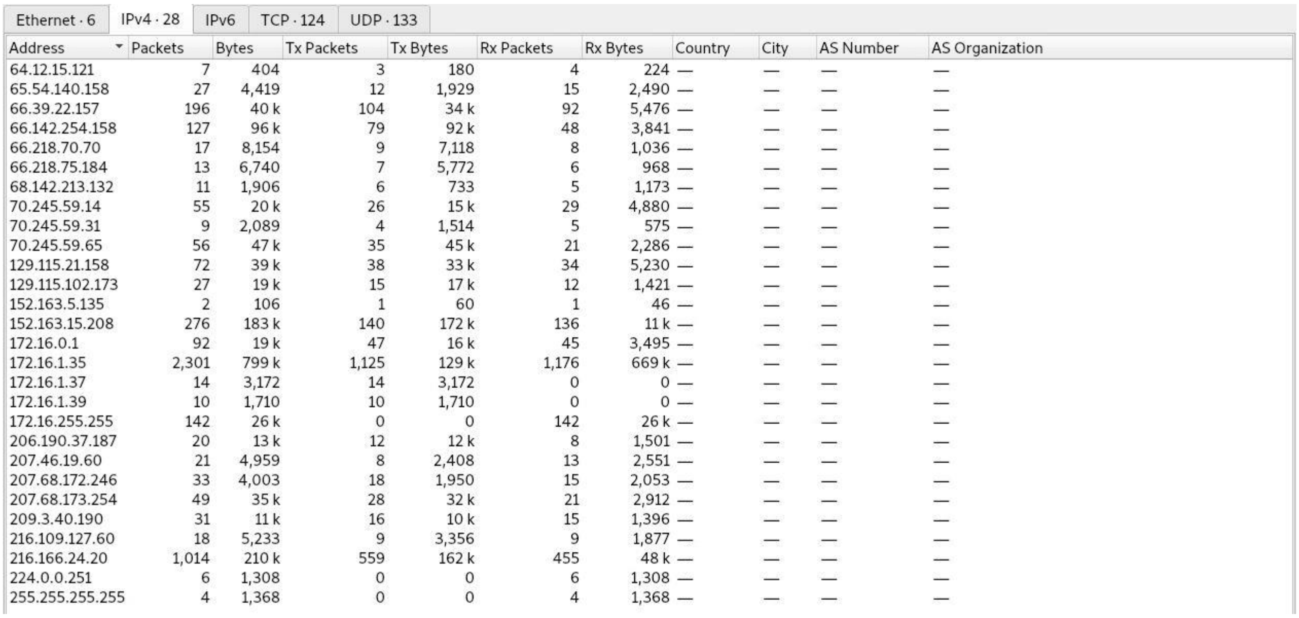


Appendix 4: Affected Device and Router information



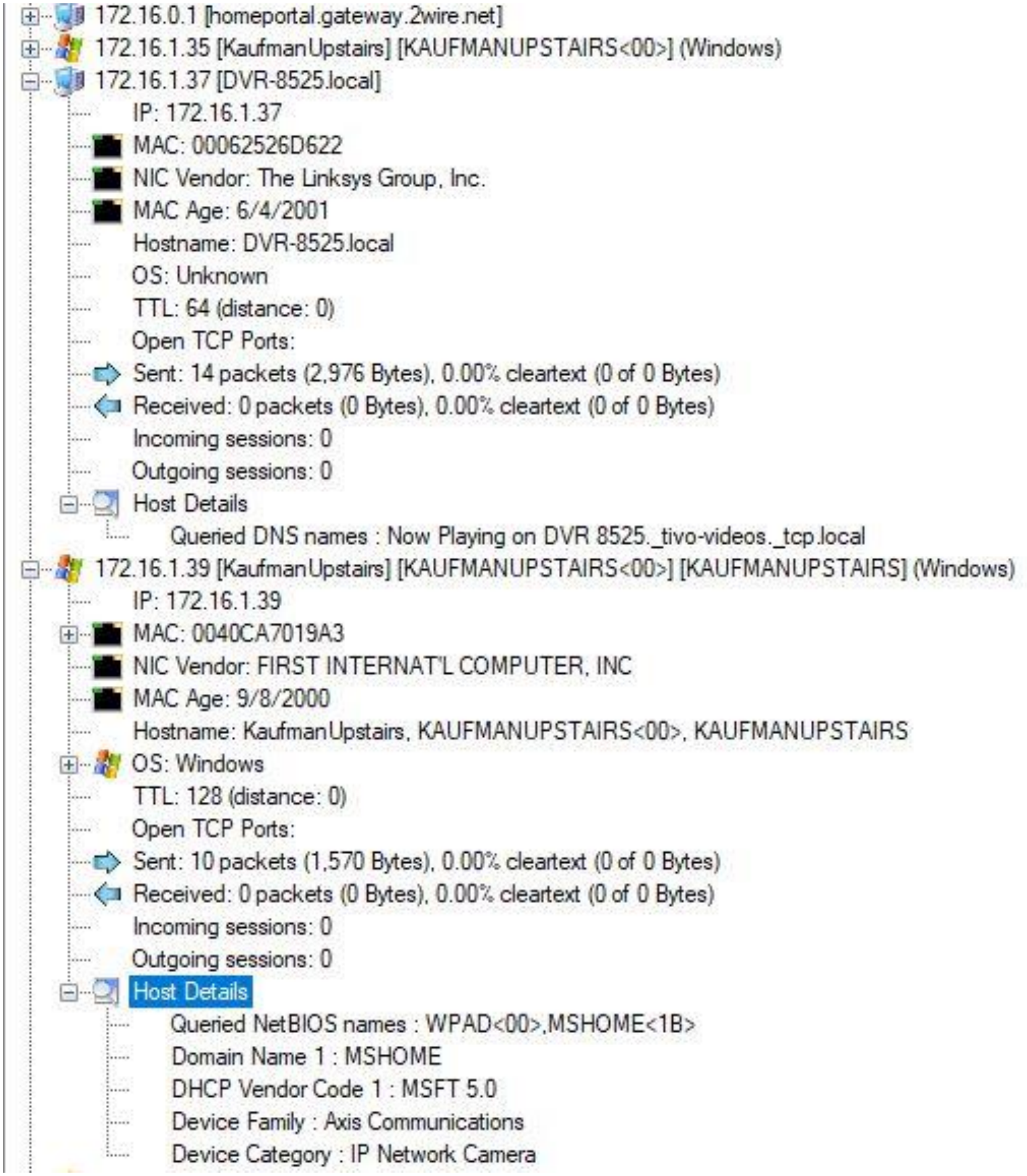
```
172.16.0.1 [homeportal.gateway.2wire.net]
    IP: 172.16.0.1
    MAC: 000D72351E11
    NIC Vendor: 2Wire Inc
    MAC Age: 6/1/2003
    Hostname: homeportal.gateway.2wire.net
    OS: Unknown
    TTL: 255 (distance: 0)
    Open TCP Ports:
    Sent: 47 packets (15,392 Bytes), 0.00% cleartext (0 of 0 Bytes)
    Received: 45 packets (2,865 Bytes), 0.00% cleartext (0 of 0 Bytes)
    Incoming sessions: 0
    Outgoing sessions: 0
    Host Details
172.16.1.35 [KaufmanUpstairs] [KAUFMANUPSTAIRS<00>] (Windows)
    IP: 172.16.1.35
    MAC: 0040CA7019A3
    NIC Vendor: FIRST INTERNAT'L COMPUTER, INC
    MAC Age: 9/8/2000
    Hostname: KaufmanUpstairs, KAUFMANUPSTAIRS<00>
    OS: Windows
        Ettercap: Windows 2000 Professional SP4 (100.00%)
        p0f (NetSA): Windows 2000 SP4, XP SP1+, 2003 [Windows] (100.00%)
        Satori DHCP: Windows - Windows XP (16.67%) Xerox WorkCentre - 7545 [Printer] [Xerox Corp.] (8.33%) Windows - Windows
        Satori TCP: Windows - Windows 7 (33.33%) Windows - Windows XP (16.67%) Windows - Windows Vista (16.67%) Windows
    TTL: 128 (distance: 0)
    Open TCP Ports:
    Sent: 1125 packets (113,766 Bytes), 0.00% cleartext (0 of 0 Bytes)
    Received: 1176 packets (650,621 Bytes), 0.00% cleartext (0 of 0 Bytes)
    Incoming sessions: 0
    Outgoing sessions: 97
    Host Details
172.16.1.37 [DVR-8525.local]
172.16.1.39 [KaufmanUpstairs] [KAUFMANUPSTAIRS<00>] [KAUFMANUPSTAIRS] (Windows)
```

Appendix 5: Packets / Bytes Breakdown



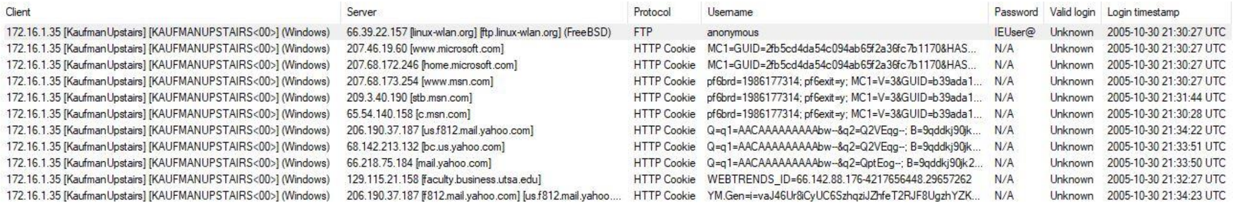
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
64.12.15.121	7	404	3	180	4	224	—	—	—	—
65.54.140.158	27	4,419	12	1,929	15	2,490	—	—	—	—
66.39.22.157	196	40 k	104	34 k	92	5,476	—	—	—	—
66.142.254.158	127	96 k	79	92 k	48	3,841	—	—	—	—
66.218.70.70	17	8,154	9	7,118	8	1,036	—	—	—	—
66.218.75.184	13	6,740	7	5,772	6	968	—	—	—	—
68.142.213.132	11	1,906	6	733	5	1,173	—	—	—	—
70.245.59.14	55	20 k	26	15 k	29	4,880	—	—	—	—
70.245.59.31	9	2,089	4	1,514	5	575	—	—	—	—
70.245.59.65	56	47 k	35	45 k	21	2,286	—	—	—	—
129.115.21.158	72	39 k	38	33 k	34	5,230	—	—	—	—
129.115.102.173	27	19 k	15	17 k	12	1,421	—	—	—	—
152.163.5.135	2	106	1	60	1	46	—	—	—	—
152.163.15.208	276	183 k	140	172 k	136	11 k	—	—	—	—
172.16.0.1	92	19 k	47	16 k	45	3,495	—	—	—	—
172.16.1.35	2,301	799 k	1,125	129 k	1,176	669 k	—	—	—	—
172.16.1.37	14	3,172	14	3,172	0	0	—	—	—	—
172.16.1.39	10	1,710	10	1,710	0	0	—	—	—	—
172.16.255.255	142	26 k	0	0	142	26 k	—	—	—	—
206.190.37.187	20	13 k	12	12 k	8	1,501	—	—	—	—
207.46.19.60	21	4,959	8	2,408	13	2,551	—	—	—	—
207.68.172.246	33	4,003	18	1,950	15	2,053	—	—	—	—
207.68.173.254	49	35 k	28	32 k	21	2,912	—	—	—	—
209.3.40.190	31	11 k	16	10 k	15	1,396	—	—	—	—
216.109.127.60	18	5,233	9	3,356	9	1,877	—	—	—	—
216.166.24.20	1,014	210 k	559	162 k	455	48 k	—	—	—	—
224.0.0.251	6	1,308	0	0	6	1,308	—	—	—	—
255.255.255.255	4	1,368	0	0	4	1,368	—	—	—	—

Appendix 6: IP Network Camera

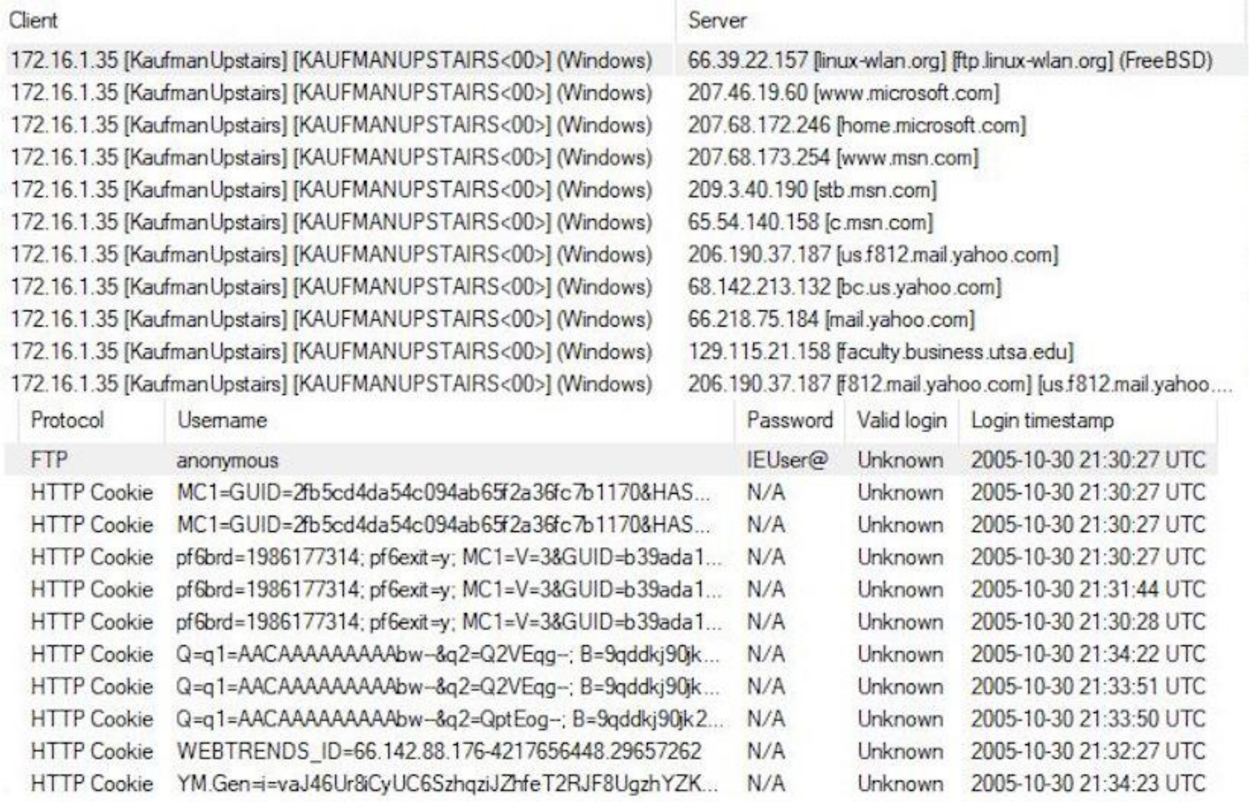


```
172.16.0.1 [homeportal.gateway.2wire.net]
172.16.1.35 [KaufmanUpstairs] [KAUFMANUPSTAIRS<00>] (Windows)
172.16.1.37 [DVR-8525.local]
    IP: 172.16.1.37
    MAC: 00062526D622
    NIC Vendor: The Linksys Group, Inc.
    MAC Age: 6/4/2001
    Hostname: DVR-8525.local
    OS: Unknown
    TTL: 64 (distance: 0)
    Open TCP Ports:
    Sent: 14 packets (2,976 Bytes), 0.00% cleartext (0 of 0 Bytes)
    Received: 0 packets (0 Bytes), 0.00% cleartext (0 of 0 Bytes)
    Incoming sessions: 0
    Outgoing sessions: 0
    Host Details
        Queried DNS names : Now Playing on DVR 8525._tivo-videos._tcp.local
172.16.1.39 [KaufmanUpstairs] [KAUFMANUPSTAIRS<00>] [KAUFMANUPSTAIRS] (Windows)
    IP: 172.16.1.39
    MAC: 0040CA7019A3
    NIC Vendor: FIRST INTERNAT'L COMPUTER, INC
    MAC Age: 9/8/2000
    Hostname: KaufmanUpstairs, KAUFMANUPSTAIRS<00>, KAUFMANUPSTAIRS
    OS: Windows
    TTL: 128 (distance: 0)
    Open TCP Ports:
    Sent: 10 packets (1,570 Bytes), 0.00% cleartext (0 of 0 Bytes)
    Received: 0 packets (0 Bytes), 0.00% cleartext (0 of 0 Bytes)
    Incoming sessions: 0
    Outgoing sessions: 0
    Host Details
        Queried NetBIOS names : WPAD<00>,MSHOME<1B>
        Domain Name 1 : MSHOME
        DHCP Vendor Code 1 : MSFT 5.0
        Device Family : Axis Communications
        Device Category : IP Network Camera
```

Appendix 7: Credentials Captured



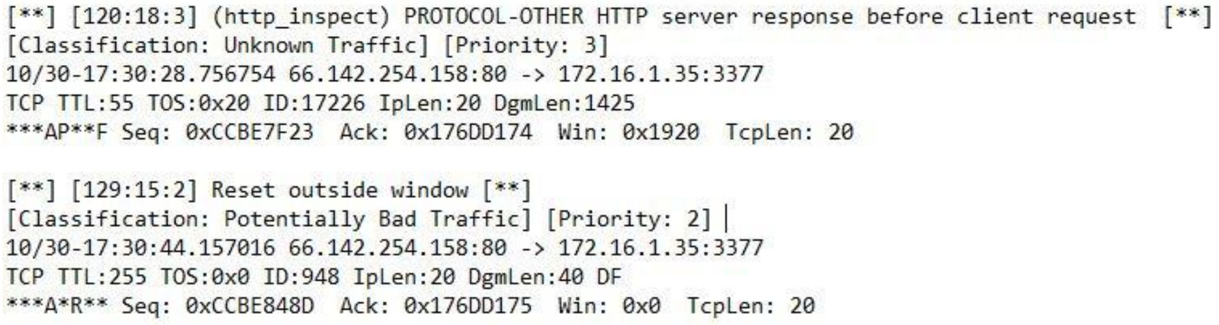
Client	Server	Protocol	Username	Password	Valid login	Login timestamp
172.16.1.35 [KaufmanUpstairs] [KAUFMANUPSTAIRS<00>] (Windows)	66.39.22.157 [linux-wlan.org] [ftp.linux-wlan.org] (FreeBSD)	FTP	anonymous	IEUser@	Unknown	2005-10-30 21:30:27 UTC
172.16.1.35 [KaufmanUpstairs] [KAUFMANUPSTAIRS<00>] (Windows)	207.46.19.60 [www.microsoft.com]	HTTP Cookie	MC1=GUID=2fb5cd4da54c094ab65f2a36fc7b1170&HAS...	N/A	Unknown	2005-10-30 21:30:27 UTC
172.16.1.35 [KaufmanUpstairs] [KAUFMANUPSTAIRS<00>] (Windows)	207.68.172.246 [home.microsoft.com]	HTTP Cookie	MC1=GUID=2fb5cd4da54c094ab65f2a36fc7b1170&HAS...	N/A	Unknown	2005-10-30 21:30:27 UTC
172.16.1.35 [KaufmanUpstairs] [KAUFMANUPSTAIRS<00>] (Windows)	207.68.173.254 [www.msn.com]	HTTP Cookie	pf6brd=1986177314; pf6exit=y; MC1=V=3&GUID=b39ada1...	N/A	Unknown	2005-10-30 21:30:27 UTC
172.16.1.35 [KaufmanUpstairs] [KAUFMANUPSTAIRS<00>] (Windows)	209.3.40.190 [stb.msn.com]	HTTP Cookie	pf6brd=1986177314; pf6exit=y; MC1=V=3&GUID=b39ada1...	N/A	Unknown	2005-10-30 21:31:44 UTC
172.16.1.35 [KaufmanUpstairs] [KAUFMANUPSTAIRS<00>] (Windows)	65.54.140.158 [c.msn.com]	HTTP Cookie	pf6brd=1986177314; pf6exit=y; MC1=V=3&GUID=b39ada1...	N/A	Unknown	2005-10-30 21:30:28 UTC
172.16.1.35 [KaufmanUpstairs] [KAUFMANUPSTAIRS<00>] (Windows)	206.190.37.187 [us.f812.mail.yahoo.com]	HTTP Cookie	Q=q1=AACAAAAAAAAAbw--&q2=Q2VEqg--; B=9qddkj90jk...	N/A	Unknown	2005-10-30 21:34:22 UTC
172.16.1.35 [KaufmanUpstairs] [KAUFMANUPSTAIRS<00>] (Windows)	68.142.213.132 [bc.us.yahoo.com]	HTTP Cookie	Q=q1=AACAAAAAAAAAbw--&q2=Q2VEqg--; B=9qddkj90jk...	N/A	Unknown	2005-10-30 21:33:51 UTC
172.16.1.35 [KaufmanUpstairs] [KAUFMANUPSTAIRS<00>] (Windows)	66.218.75.184 [mail.yahoo.com]	HTTP Cookie	Q=q1=AACAAAAAAAAAbw--&q2=QptEog--; B=9qddkj90jk2...	N/A	Unknown	2005-10-30 21:33:50 UTC
172.16.1.35 [KaufmanUpstairs] [KAUFMANUPSTAIRS<00>] (Windows)	129.115.21.158 [faculty.business.utsa.edu]	HTTP Cookie	WEBTRENDS_ID=66.142.88.176-4217656448.29657262	N/A	Unknown	2005-10-30 21:32:27 UTC
172.16.1.35 [KaufmanUpstairs] [KAUFMANUPSTAIRS<00>] (Windows)	206.190.37.187 [f812.mail.yahoo.com] [us.f812.mail.yahoo....	HTTP Cookie	YM.Gen=i=vaJ46Ur8iCyUC6SzhqziJZhfeT2RJF8UgzhYZK...	N/A	Unknown	2005-10-30 21:34:23 UTC



Client	Server
172.16.1.35 [KaufmanUpstairs] [KAUFMANUPSTAIRS<00>] (Windows)	66.39.22.157 [linux-wlan.org] [ftp.linux-wlan.org] (FreeBSD)
172.16.1.35 [KaufmanUpstairs] [KAUFMANUPSTAIRS<00>] (Windows)	207.46.19.60 [www.microsoft.com]
172.16.1.35 [KaufmanUpstairs] [KAUFMANUPSTAIRS<00>] (Windows)	207.68.172.246 [home.microsoft.com]
172.16.1.35 [KaufmanUpstairs] [KAUFMANUPSTAIRS<00>] (Windows)	207.68.173.254 [www.msn.com]
172.16.1.35 [KaufmanUpstairs] [KAUFMANUPSTAIRS<00>] (Windows)	209.3.40.190 [stb.msn.com]
172.16.1.35 [KaufmanUpstairs] [KAUFMANUPSTAIRS<00>] (Windows)	65.54.140.158 [c.msn.com]
172.16.1.35 [KaufmanUpstairs] [KAUFMANUPSTAIRS<00>] (Windows)	206.190.37.187 [us.f812.mail.yahoo.com]
172.16.1.35 [KaufmanUpstairs] [KAUFMANUPSTAIRS<00>] (Windows)	68.142.213.132 [bc.us.yahoo.com]
172.16.1.35 [KaufmanUpstairs] [KAUFMANUPSTAIRS<00>] (Windows)	66.218.75.184 [mail.yahoo.com]
172.16.1.35 [KaufmanUpstairs] [KAUFMANUPSTAIRS<00>] (Windows)	129.115.21.158 [faculty.business.utsa.edu]
172.16.1.35 [KaufmanUpstairs] [KAUFMANUPSTAIRS<00>] (Windows)	206.190.37.187 [f812.mail.yahoo.com] [us.f812.mail.yahoo....

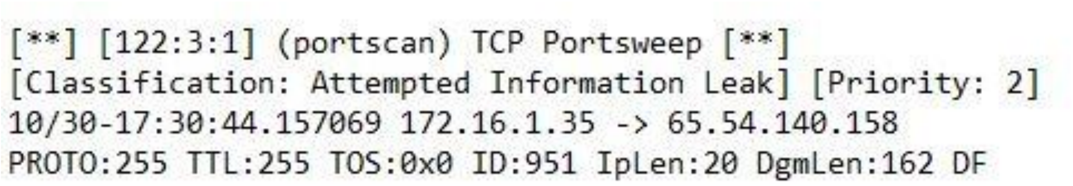
Protocol	Username	Password	Valid login	Login timestamp
FTP	anonymous	IEUser@	Unknown	2005-10-30 21:30:27 UTC
HTTP Cookie	MC1=GUID=2fb5cd4da54c094ab65f2a36fc7b1170&HAS...	N/A	Unknown	2005-10-30 21:30:27 UTC
HTTP Cookie	MC1=GUID=2fb5cd4da54c094ab65f2a36fc7b1170&HAS...	N/A	Unknown	2005-10-30 21:30:27 UTC
HTTP Cookie	pf6brd=1986177314; pf6exit=y; MC1=V=3&GUID=b39ada1...	N/A	Unknown	2005-10-30 21:30:27 UTC
HTTP Cookie	pf6brd=1986177314; pf6exit=y; MC1=V=3&GUID=b39ada1...	N/A	Unknown	2005-10-30 21:31:44 UTC
HTTP Cookie	pf6brd=1986177314; pf6exit=y; MC1=V=3&GUID=b39ada1...	N/A	Unknown	2005-10-30 21:30:28 UTC
HTTP Cookie	Q=q1=AACAAAAAAAAAbw--&q2=Q2VEqg--; B=9qddkj90jk...	N/A	Unknown	2005-10-30 21:34:22 UTC
HTTP Cookie	Q=q1=AACAAAAAAAAAbw--&q2=Q2VEqg--; B=9qddkj90jk...	N/A	Unknown	2005-10-30 21:33:51 UTC
HTTP Cookie	Q=q1=AACAAAAAAAAAbw--&q2=QptEog--; B=9qddkj90jk2...	N/A	Unknown	2005-10-30 21:33:50 UTC
HTTP Cookie	WEBTRENDS_ID=66.142.88.176-4217656448.29657262	N/A	Unknown	2005-10-30 21:32:27 UTC
HTTP Cookie	YM.Gen=i=vaJ46Ur8iCyUC6SzhqziJZhfeT2RJF8UgzhYZK...	N/A	Unknown	2005-10-30 21:34:23 UTC

Appendix 8: Snort Other HTTP Server



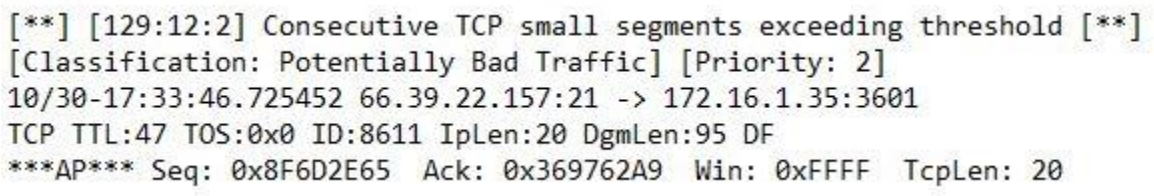
```
[**] [120:18:3] (http_inspect) PROTOCOL-OTHER HTTP server response before client request  [**]
[Classification: Unknown Traffic] [Priority: 3]
10/30-17:30:28.756754 66.142.254.158:80 -> 172.16.1.35:3377
TCP TTL:55 TOS:0x20 ID:17226 IpLen:20 DgmLen:1425
***AP**F Seq: 0xCCBE7F23  Ack: 0x176DD174  Win: 0x1920  TcpLen: 20

[**] [129:15:2] Reset outside window [**]
[Classification: Potentially Bad Traffic] [Priority: 2] |
10/30-17:30:44.157016 66.142.254.158:80 -> 172.16.1.35:3377
TCP TTL:255 TOS:0x0 ID:948 IpLen:20 DgmLen:40 DF
***A*R** Seq: 0xCCBE848D  Ack: 0x176DD175  Win: 0x0  TcpLen: 20
```

Appendix 9: Snort TCP Portsweep



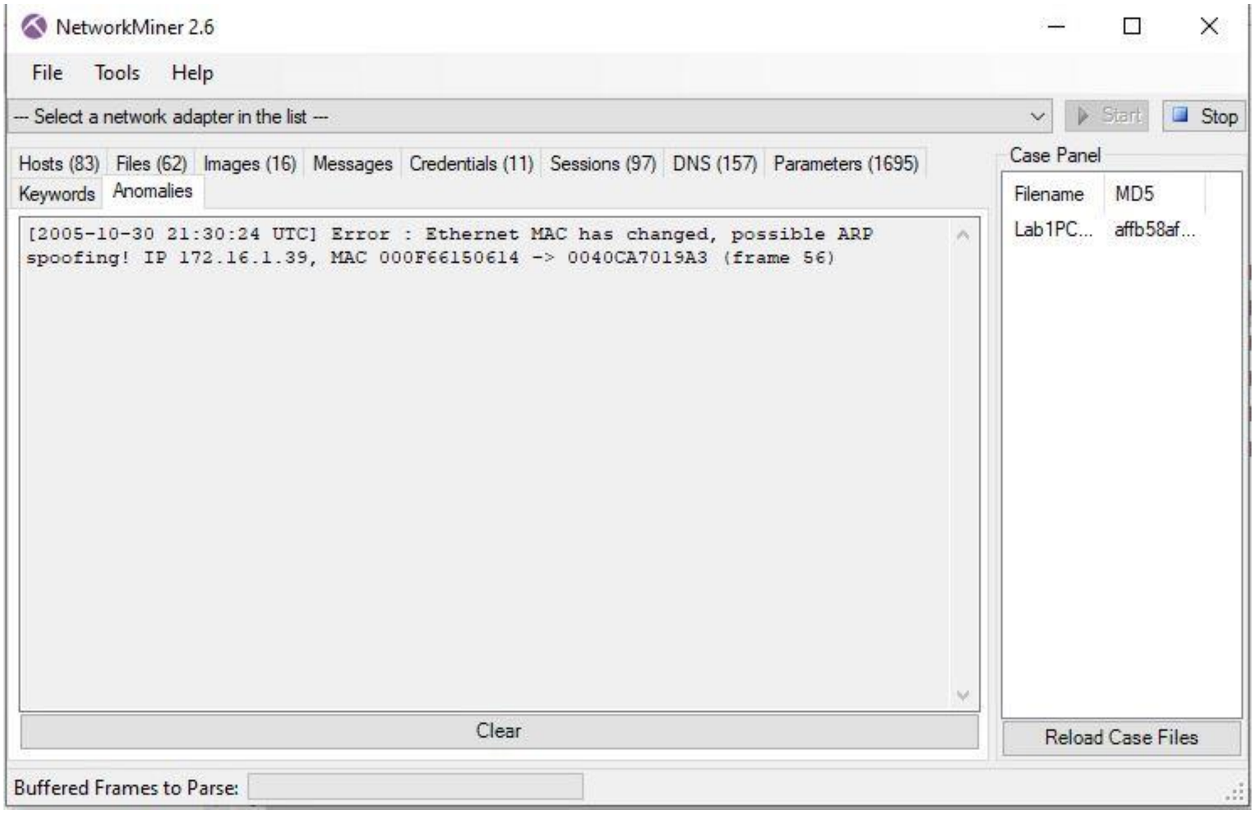
```
[**] [122:3:1] (portscan) TCP Portsweep [**]
[Classification: Attempted Information Leak] [Priority: 2]
10/30-17:30:44.157069 172.16.1.35 -> 65.54.140.158
PROTO:255 TTL:255 TOS:0x0 ID:951 IpLen:20 DgmLen:162 DF
```

Appendix 10: Snort TCP Small Segment Threshold



```
[**] [129:12:2] Consecutive TCP small segments exceeding threshold [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
10/30-17:33:46.725452 66.39.22.157:21 -> 172.16.1.35:3601
TCP TTL:47 TOS:0x0 ID:8611 IpLen:20 DgmLen:95 DF
***AP*** Seq: 0x8F6D2E65  Ack: 0x369762A9  Win: 0xFFFF  TcpLen: 20
```

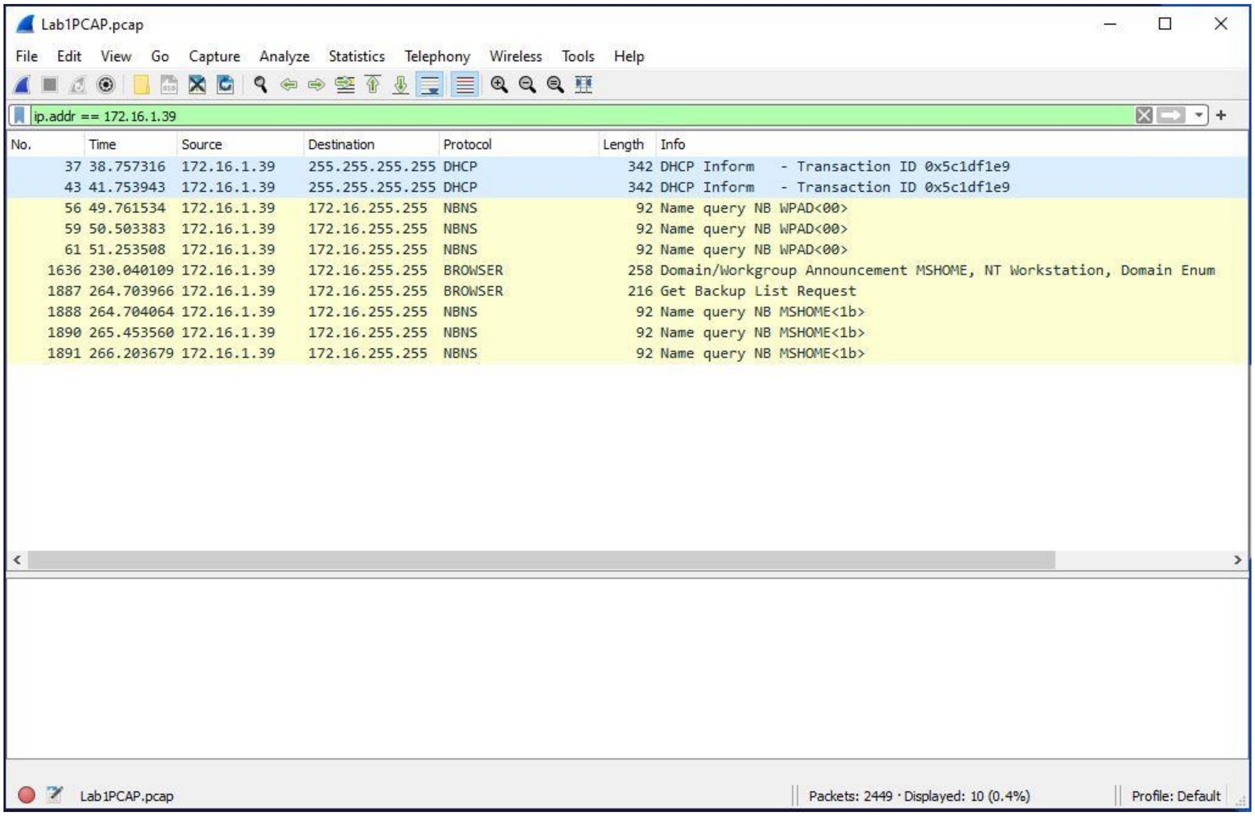
Appendix 11: NetworkMiner ARP Spoofing



```
[2005-10-30 21:30:24 UTC] Error : Ethernet MAC has changed, possible ARP
spoofing! IP 172.16.1.39, MAC 000F66150614 -> 0040CA7019A3 (frame 56)
```

Filename	MD5
Lab1PC...	affb58af...

Appendix 12: 172.16.1.39 Packets

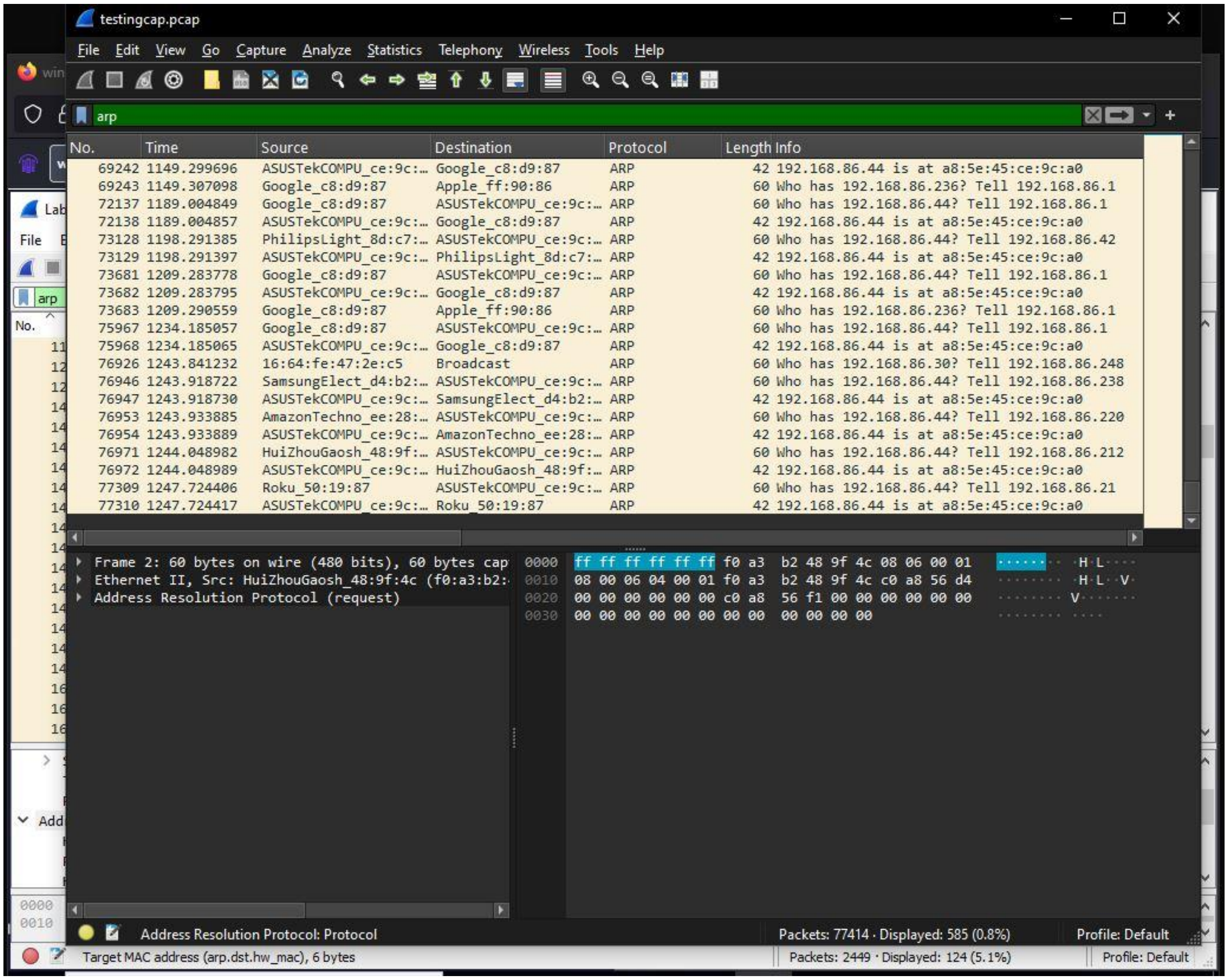

Lab1PCAP.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 172.16.1.39

```
No.     Time       Source         Destination     Protocol         Length Info
     37 38.757316  172.16.1.39    255.255.255.255 DHCP                342 DHCP Inform   - Transaction ID 0x5c1df1e9
     43 41.753943  172.16.1.39    255.255.255.255 DHCP                342 DHCP Inform   - Transaction ID 0x5c1df1e9
     56 49.761534  172.16.1.39    172.16.255.255  NBNS                 92 Name query NB WPAD<00>
     59 50.503383  172.16.1.39    172.16.255.255  NBNS                 92 Name query NB WPAD<00>
     61 51.253508  172.16.1.39    172.16.255.255  NBNS                 92 Name query NB WPAD<00>
   1636 230.040109 172.16.1.39    172.16.255.255  BROWSER             258 Domain/Workgroup Announcement MSHOME, NT Workstation, Domain Enum
   1887 264.703966 172.16.1.39    172.16.255.255  BROWSER             216 Get Backup List Request
   1888 264.704064 172.16.1.39    172.16.255.255  NBNS                 92 Name query NB MSHOME<1b>
   1890 265.453560 172.16.1.39    172.16.255.255  NBNS                 92 Name query NB MSHOME<1b>
   1891 266.203679 172.16.1.39    172.16.255.255  NBNS                 92 Name query NB MSHOME<1b>
```

Lab1PCAP.pcap | Packets: 2449 · Displayed: 10 (0.4%) | Profile: Default

Appendix 13: Gratuitous ARP packets


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

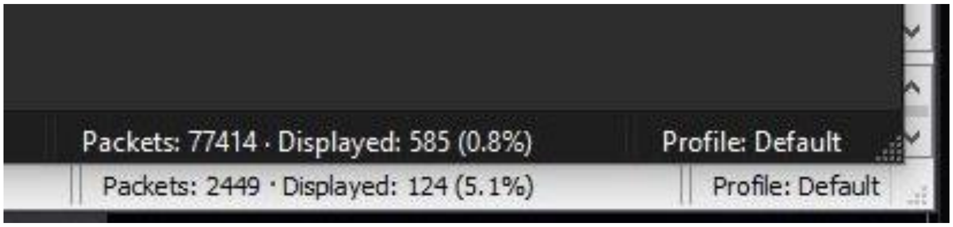
```
No.   Time        Source                 Destination            Protocol Length Info
69242 1149.299696 ASUSTekCOMPU_ce:9c:…   Google_c8:d9:87        ARP      42 192.168.86.44 is at a8:5e:45:ce:9c:a0
69243 1149.307098 Google_c8:d9:87        Apple_ff:90:86         ARP      60 Who has 192.168.86.236? Tell 192.168.86.1
72137 1189.004849 Google_c8:d9:87        ASUSTekCOMPU_ce:9c:…   ARP      60 Who has 192.168.86.44? Tell 192.168.86.1
72138 1189.004857 ASUSTekCOMPU_ce:9c:…   Google_c8:d9:87        ARP      42 192.168.86.44 is at a8:5e:45:ce:9c:a0
73128 1198.291385 PhilipsLight_8d:c7:…   ASUSTekCOMPU_ce:9c:…   ARP      60 Who has 192.168.86.44? Tell 192.168.86.42
73129 1198.291397 ASUSTekCOMPU_ce:9c:…   PhilipsLight_8d:c7:…   ARP      42 192.168.86.44 is at a8:5e:45:ce:9c:a0
73681 1209.283778 Google_c8:d9:87        ASUSTekCOMPU_ce:9c:…   ARP      60 Who has 192.168.86.44? Tell 192.168.86.1
73682 1209.283795 ASUSTekCOMPU_ce:9c:…   Google_c8:d9:87        ARP      42 192.168.86.44 is at a8:5e:45:ce:9c:a0
73683 1209.290559 Google_c8:d9:87        Apple_ff:90:86         ARP      60 Who has 192.168.86.236? Tell 192.168.86.1
75967 1234.185057 Google_c8:d9:87        ASUSTekCOMPU_ce:9c:…   ARP      60 Who has 192.168.86.44? Tell 192.168.86.1
75968 1234.185065 ASUSTekCOMPU_ce:9c:…   Google_c8:d9:87        ARP      42 192.168.86.44 is at a8:5e:45:ce:9c:a0
76926 1243.841232 16:64:fe:47:2e:c5      Broadcast              ARP      60 Who has 192.168.86.30? Tell 192.168.86.248
76946 1243.918722 SamsungElect_d4:b2:…   ASUSTekCOMPU_ce:9c:…   ARP      60 Who has 192.168.86.44? Tell 192.168.86.238
76947 1243.918730 ASUSTekCOMPU_ce:9c:…   SamsungElect_d4:b2:…   ARP      42 192.168.86.44 is at a8:5e:45:ce:9c:a0
76953 1243.933885 AmazonTechno_ee:28:…   ASUSTekCOMPU_ce:9c:…   ARP      60 Who has 192.168.86.44? Tell 192.168.86.220
76954 1243.933889 ASUSTekCOMPU_ce:9c:…   AmazonTechno_ee:28:…   ARP      42 192.168.86.44 is at a8:5e:45:ce:9c:a0
76971 1244.048982 HuiZhouGaosh_48:9f:…   ASUSTekCOMPU_ce:9c:…   ARP      60 Who has 192.168.86.44? Tell 192.168.86.212
76972 1244.048989 ASUSTekCOMPU_ce:9c:…   HuiZhouGaosh_48:9f:…   ARP      42 192.168.86.44 is at a8:5e:45:ce:9c:a0
77309 1247.724406 Roku_50:19:87          ASUSTekCOMPU_ce:9c:…   ARP      60 Who has 192.168.86.44? Tell 192.168.86.21
77310 1247.724417 ASUSTekCOMPU_ce:9c:…   Roku_50:19:87          ARP      42 192.168.86.44 is at a8:5e:45:ce:9c:a0
```

```
> Frame 2: 60 bytes on wire (480 bits), 60 bytes cap
> Ethernet II, Src: HuiZhouGaosh_48:9f:4c (f0:a3:b2:
> Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff f0 a3  b2 48 9f 4c 08 06 00 01   ········ ·H·L····
0010  08 00 06 04 00 01 f0 a3  b2 48 9f 4c c0 a8 56 d4   ········ ·H·L··V·
0020  00 00 00 00 00 00 c0 a8  56 f1 00 00 00 00 00 00   ········ V·······
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

Address Resolution Protocol: Protocol | Packets: 77414 · Displayed: 585 (0.8%) | Profile: Default

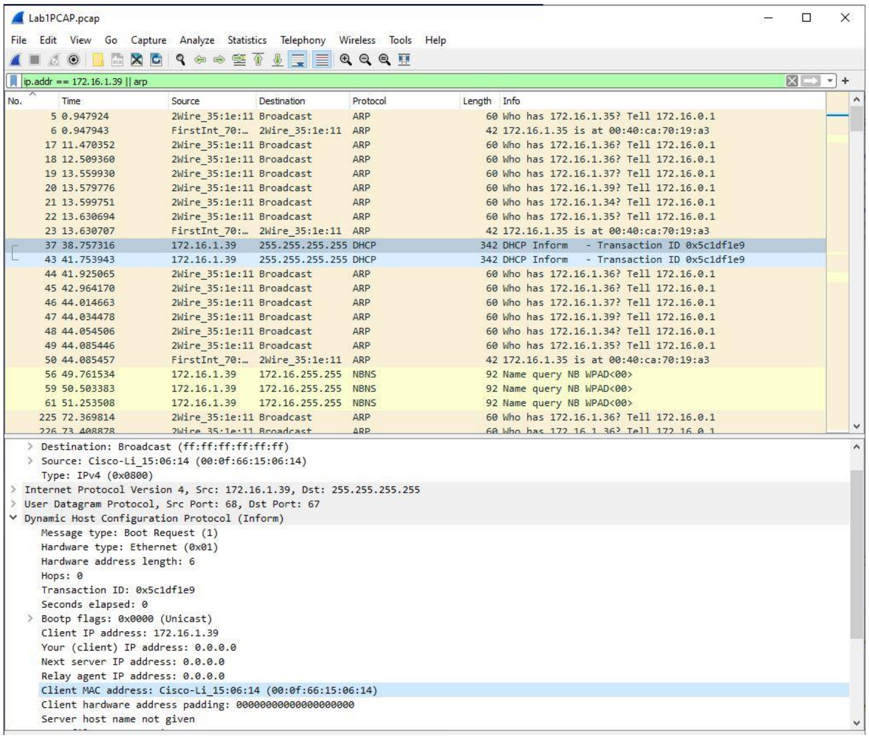
Target MAC address (arp.dst.hw_mac), 6 bytes | Packets: 2449 · Displayed: 124 (5.1%) | Profile: Default



Packets: 77414 · Displayed: 585 (0.8%) Profile: Default

Packets: 2449 · Displayed: 124 (5.1%) Profile: Default

Appendix 14: Prior MAC amidst ARP Flood

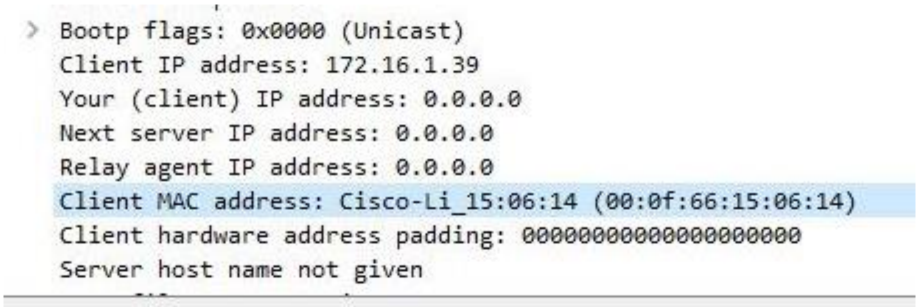


Lab1PCAP.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

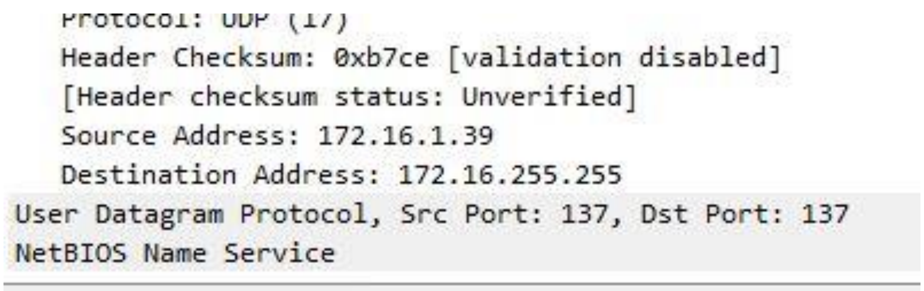
```
ip.addr == 172.16.1.39 || arp
```

```
No.   Time        Source            Destination      Protocol  Length Info
    5 0.947924    2Wire_35:1e:11 Broadcast        ARP           60 Who has 172.16.1.35? Tell 172.16.0.1
    6 0.947943    FirstInt_70:…  2Wire_35:1e:11   ARP           42 172.16.1.35 is at 00:40:ca:70:19:a3
   17 11.470352   2Wire_35:1e:11 Broadcast        ARP           60 Who has 172.16.1.36? Tell 172.16.0.1
   18 12.509360   2Wire_35:1e:11 Broadcast        ARP           60 Who has 172.16.1.36? Tell 172.16.0.1
   19 13.559930   2Wire_35:1e:11 Broadcast        ARP           60 Who has 172.16.1.37? Tell 172.16.0.1
   20 13.579776   2Wire_35:1e:11 Broadcast        ARP           60 Who has 172.16.1.39? Tell 172.16.0.1
   21 13.599751   2Wire_35:1e:11 Broadcast        ARP           60 Who has 172.16.1.34? Tell 172.16.0.1
   22 13.630694   2Wire_35:1e:11 Broadcast        ARP           60 Who has 172.16.1.35? Tell 172.16.0.1
   23 13.630707   FirstInt_70:…  2Wire_35:1e:11   ARP           42 172.16.1.35 is at 00:40:ca:70:19:a3
   37 38.757316   172.16.1.39    255.255.255.255 DHCP         342 DHCP Inform   - Transaction ID 0x5c1df1e9
   43 41.753943   172.16.1.39    255.255.255.255 DHCP         342 DHCP Inform   - Transaction ID 0x5c1df1e9
   44 41.925065   2Wire_35:1e:11 Broadcast        ARP           60 Who has 172.16.1.36? Tell 172.16.0.1
   45 42.964170   2Wire_35:1e:11 Broadcast        ARP           60 Who has 172.16.1.36? Tell 172.16.0.1
   46 44.014663   2Wire_35:1e:11 Broadcast        ARP           60 Who has 172.16.1.37? Tell 172.16.0.1
   47 44.034478   2Wire_35:1e:11 Broadcast        ARP           60 Who has 172.16.1.39? Tell 172.16.0.1
   48 44.054506   2Wire_35:1e:11 Broadcast        ARP           60 Who has 172.16.1.34? Tell 172.16.0.1
   49 44.085446   2Wire_35:1e:11 Broadcast        ARP           60 Who has 172.16.1.35? Tell 172.16.0.1
   50 44.085457   FirstInt_70:…  2Wire_35:1e:11   ARP           42 172.16.1.35 is at 00:40:ca:70:19:a3
   56 49.761534   172.16.1.39    172.16.255.255   NBNS          92 Name query NB WPAD<00>
   59 50.503383   172.16.1.39    172.16.255.255   NBNS          92 Name query NB WPAD<00>
   61 51.253508   172.16.1.39    172.16.255.255   NBNS          92 Name query NB WPAD<00>
  225 72.369814   2Wire_35:1e:11 Broadcast        ARP           60 Who has 172.16.1.36? Tell 172.16.0.1
  226 73.408878   2Wire_35:1e:11 Broadcast        ARP           60 Who has 172.16.1.36? Tell 172.16.0.1
```

```
   > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
   > Source: Cisco-Li_15:06:14 (00:0f:66:15:06:14)
     Type: IPv4 (0x0800)
 > Internet Protocol Version 4, Src: 172.16.1.39, Dst: 255.255.255.255
 > User Datagram Protocol, Src Port: 68, Dst Port: 67
 v Dynamic Host Configuration Protocol (Inform)
     Message type: Boot Request (1)
     Hardware type: Ethernet (0x01)
     Hardware address length: 6
     Hops: 0
     Transaction ID: 0x5c1df1e9
     Seconds elapsed: 0
   > Bootp flags: 0x0000 (Unicast)
     Client IP address: 172.16.1.39
     Your (client) IP address: 0.0.0.0
     Next server IP address: 0.0.0.0
     Relay agent IP address: 0.0.0.0
     Client MAC address: Cisco-Li_15:06:14 (00:0f:66:15:06:14)
     Client hardware address padding: 00000000000000000000
     Server host name not given
```



```
 > Bootp flags: 0x0000 (Unicast)
   Client IP address: 172.16.1.39
   Your (client) IP address: 0.0.0.0
   Next server IP address: 0.0.0.0
   Relay agent IP address: 0.0.0.0
   Client MAC address: Cisco-Li_15:06:14 (00:0f:66:15:06:14)
   Client hardware address padding: 00000000000000000000
   Server host name not given
```



```
   Protocol: UDP (17)
   Header Checksum: 0xb7ce [validation disabled]
   [Header checksum status: Unverified]
   Source Address: 172.16.1.39
   Destination Address: 172.16.255.255
User Datagram Protocol, Src Port: 137, Dst Port: 137
NetBIOS Name Service
```