University of Texas at San Antonio

Identifying Suspicious Network Events In Captured Traffic

Daniella Carbuccia

IS 3523: Intrusion Detection and Incident Response

21 Sept. 2025

In cybersecurity, every packet of data sent across a network can have the potential to reveal critical information such as system vulnerabilities, user behavior, or even an ongoing attack. Therefore, packet capture analysis is essential for cybersecurity professionals to know to identify malicious activity and reconstruct events on a network. This lab contained a PCAP file through Sim Space, where the user suspected that something unusual happened while browsing the internet. Although the user typically relies on the network for basic email access, the capture provided evidence that more activity occurred beyond email usage.

The purpose of this report is to analyze the PCAP using Wireshark, NetworkMiner, and SNORT. Wireshark was used to examine packet details, NetworkMiner provided higher-level details such as files and credentials, and Snort acted as an intrusion detection system to look for common attack signatures. With all of these tools, it made it possible to answer key questions including the length of the packet capture, the protocols that were used, what devices were on the network, and if the traffic had any signs of malicious behavior. The main objective was to see if the user's suspicions were justified, and to find a narrative or story of what occurred during the session.

When the capture was conducted, it spanned just over eight minutes in length. Wireshark recorded a total of 2,449 packets and approximately 811,157 bytes of traffic (see Appendix A, Figure 1). From the start, it was evident that TCP was the main driver in the session, representing almost 85 percent of all packets. Some other protocols were HTTP, FTP and TLS. Since HTTP and FTP were found in the capture, it highlighted some potential risks, as plaintext communication can expose credentials and session tokens. TLS, however, represented attempts at more secure exchanges.

In order to see where majority of the traffic happened, I looked at the I/O Graph in Wireshark and noticed a significant traffic spike between 93 and 98 seconds (Appendix A, Figure 2). During that short amount of time, the volume of packets and bytes exceeded the baseline by a lot. When I filtered these packets, it revealed that the spike corresponded to the retrieval of multiple HTTP objects from external servers. In these objects it contained banner images, JavaScript files, and Flash objects, which are usually associated with online advertising. Although advertising is common with websites, they are also frequently used for malicious activity.

Through looking into the endpoints, I was able to see where this traffic originated from. The host machine connected to Microsoft MSN services, Yahoo, AOL, and a UTSA Faculty Business server (Appendix A, Figure 3). These connections reflected normal browsing activity the student described in the assignment such as checking their email and accessing university resources. However, the host also communicated with advertising and third-party servers. These contained suspicious files such as slideimages_header.js, which contained JavaScript designed to open pop-ups and redirect users (Appendix A, Figure 4). There were also several Shockwave Flash files that were downloaded, which raised additional concern.

NetworkMiner was able to provide context by identifying the host machine as "KaufmanUpstairs", the IP address as 172.16.1.35, and the operating system as Windows OS. (Appendix A, Figure 5). NetworkMiner also revealed other devices that were present on the local network such as DVR-8525.local at 172.16.1.37, the router gateway at 172.16.0.1, and a second KaufmanUpstairs at 172.16.1.39. The subnet was a typical 172.16.1.0/24 private home network. There was also no evidence that the main host attempted to access the DVR or the second

KaufmanUpstairs system directly. Any communications with these devices were limited to broadcast and ARP traffic which is typical behavior on a LAN.

Despite this, NetworkMiner flagged an anomaly that raised red flags. At frame 56, the MAC address for 172.16.1.39 changed unexpectedly, which is consistent with ARP spoofing (Appendix A, Figure 6). This could indicate an attempt to conduct a man-in-the-middle attack, where an attacker puts themselves between the host and the gateway to intercept or manipulate traffic. While one isolated anomaly doesn't confirm a successful attack, it raises concern when JavaScript and Flash content were also observed earlier.

I attempted to test the PCAP with Snort, but it only returned warnings about missing preprocessors, and I didn't see any alerts. I believe this was an error on my part as I did not have an easy time working with this tool, but I did have enough information from the other tools that were used in this lab that indicated suspicious activity. The automated detection alone is not sufficient enough for comprehensive analysis, but it would've been a good clue to confirm suspicious activity.

The evidence from the capture shows that it began with legitimate browsing activity but quickly introduced risks through advertising and insecure protocols. The large amount of traffic between 93 and 98 seconds showed how a single moment of web activity can flood the network with potentially dangerous objects. Scripts and Flash files are not always malicious, but their presence in the capture represents real-world attack methods where malvertising campaigns are embedded into legitimate web pages.

One of the most concerning discoveries came when I analyzed the JavaScript file retrieved during the spike. The code had instructions to check if the hostname included "www.rbfcu.org." If not, it would replace the hostname and open a new browser pointing to what appeared to be legitimate RBFCU resources. However, it didn't originate from RBFCU's legitimate servers. The content was actually hosted on a FreeBSD server at 216.166.24.20 IP address, and it was delivered over HTTP which is unencrypted. This possibly indicates a fake RBFCU redirect. This is often used in phishing or malvertising campaigns to attract users to interact with fake websites that mimic trusted ones. (See Appendix, Figure 7.)

The ARP spoofing was another critical factor in understanding the network's state. Even though there was no evidence that it led to compromised traffic, it is concerning. Man-in-the-middle attacks are one of the most common techniques attackers use to steal credentials or inject malicious payloads into otherwise secure sessions. The insecure HTTP traffic, spoofing attempt, suspicious script behavior, and the fake RBFCU redirect, created a scenario where the user was at risk, even if we didn't witness a complete compromise.

This lab demonstrates how everyday browsing can intersect with threats. Users often assume that visiting familiar sites and checking email is safe but through this lab it demonstrated that even normal actions can carry hidden risks. For professionals it is clear that you can't just be vigilant with obvious threats or high-profile attacks. Instead, every network interaction must be viewed through magnifying glass and as a potential point of exploitation.

The analysis of the PCAP demonstrated that a seemingly normal browsing session had several suspicious elements. Although the user visited their typical services such as MSN, Yahoo, AOL, and UTSA, the traffic also had suspicious advertising content, JavaScript, Flash files, and a redirect attempt to a fraudulent RBFCU site. NetworkMiner's warning of ARP spoofing further suggested a possible man-in-the-middle attack. Although I couldn't retrieve any alerts with Snort, Wireshark and NetworkMiner showed in many ways that the environment was not completely safe. This lab showed that even normal internet usage poses risks, and that layered analysis can be very helpful in uncovering them.

References

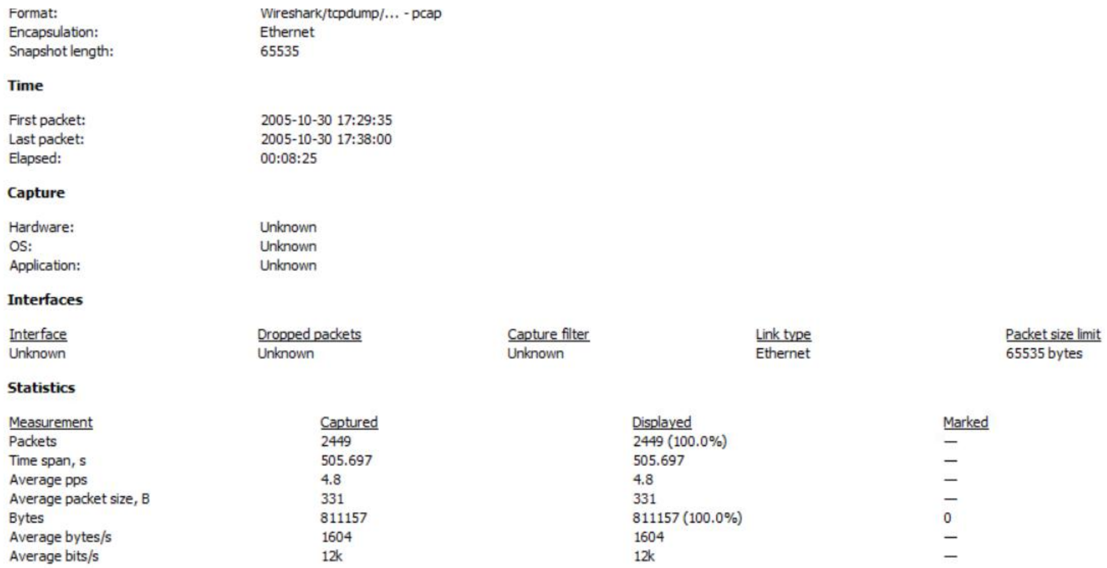
Manipulator-in-the-middle attack. OWASP Foundation. (n.d.). https://owasp.org/www-community/attacks/Manipulator-in-the-middle_attack

What is malvertising and how to prevent it?. Fortinet. (n.d.). https://www.fortinet.com/resources/cyberglossary/malvertising

Appendices

Appendix A

Figure 1.



Format:	Wireshark/tcpdump/... - pcap
Encapsulation:	Ethernet
Snapshot length:	65535

Time

First packet:	2005-10-30 17:29:35
Last packet:	2005-10-30 17:38:00
Elapsed:	00:08:25

Capture

Hardware:	Unknown
OS:	Unknown
Application:	Unknown

Interfaces

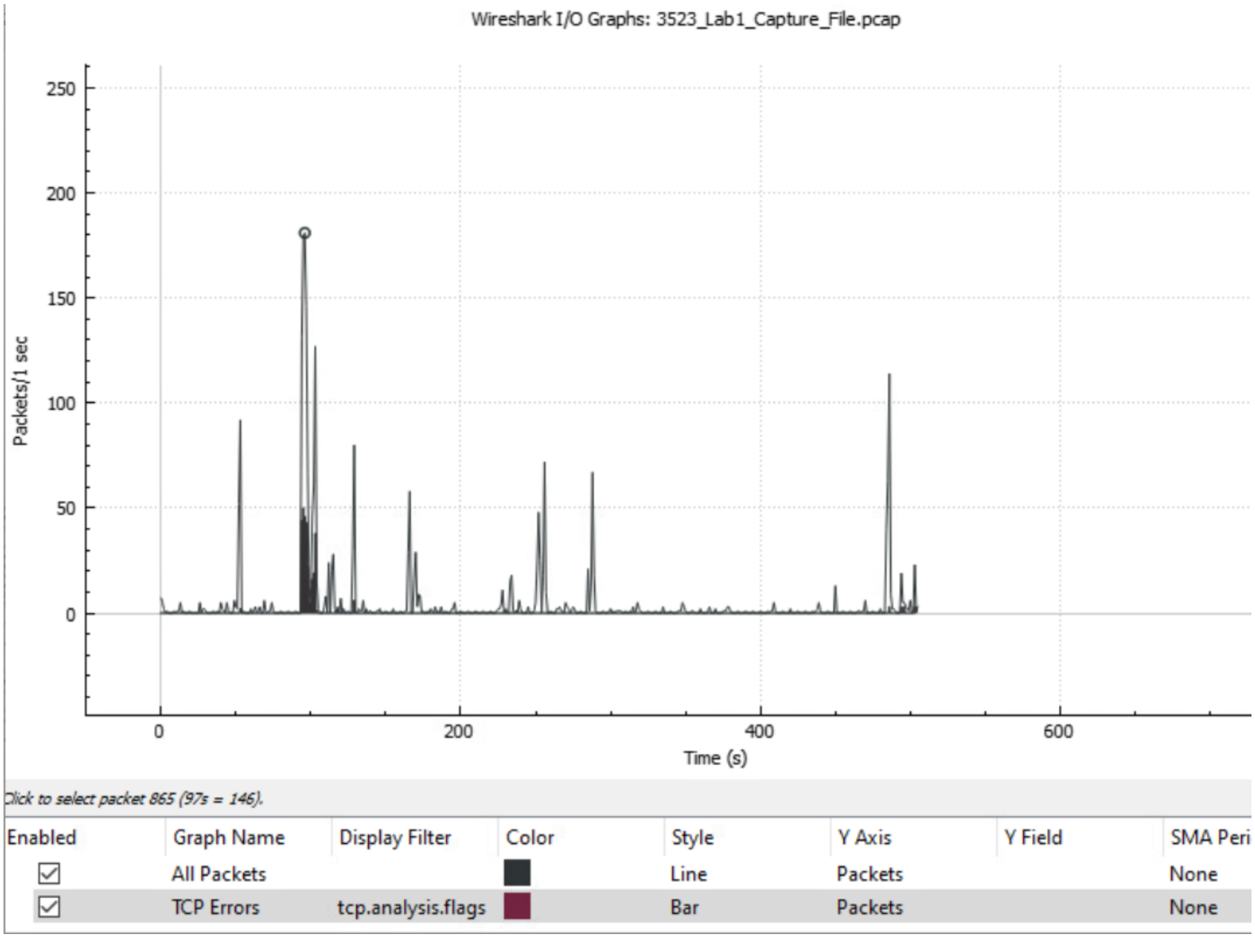
Interface	Dropped packets	Capture filter	Link type	Packet size limit
Unknown	Unknown	Unknown	Ethernet	65535 bytes

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	1604	1604	—
Average bits/s	12k	12k	—

Wireshark statistics showing 2,449 packets and 811,157 bytes.

Figure 2

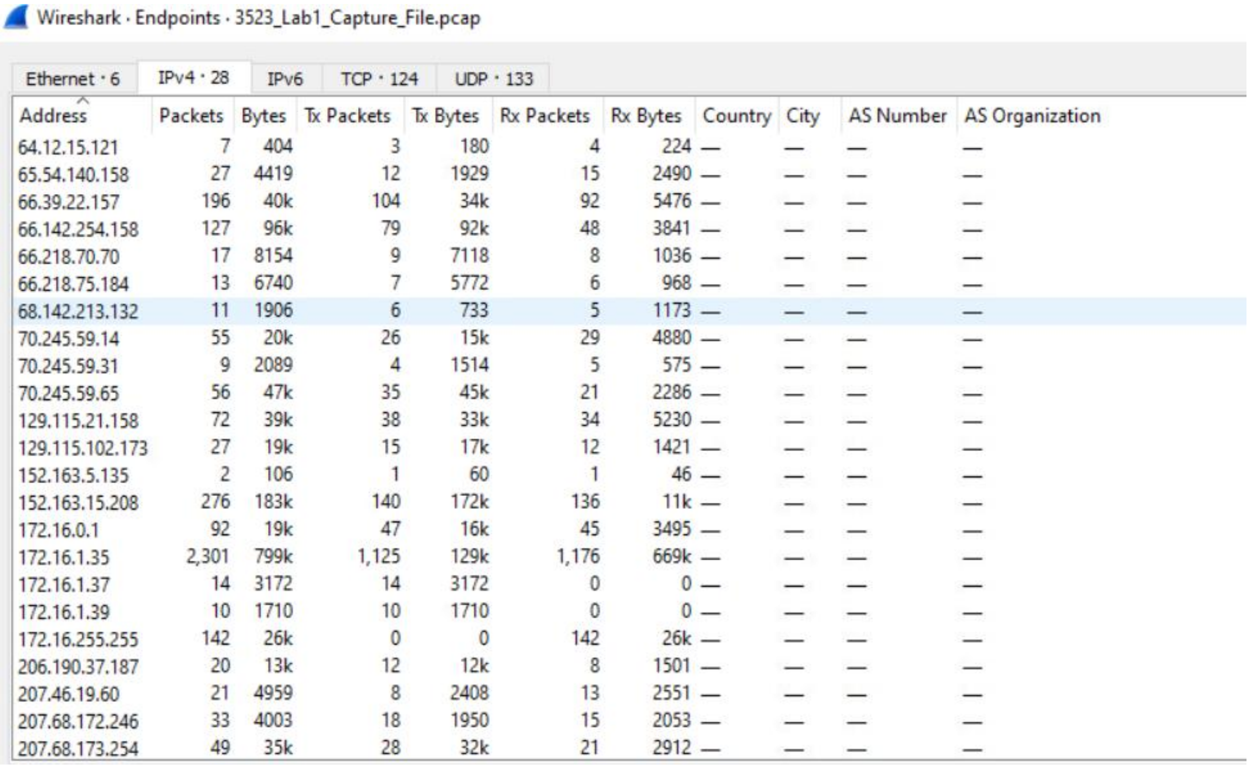


Click to select packet 865 (97s = 146).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Peri
☑	All Packets		■	Line	Packets		None
☑	TCP Errors	tcp.analysis.flags	🟥	Bar	Packets		None

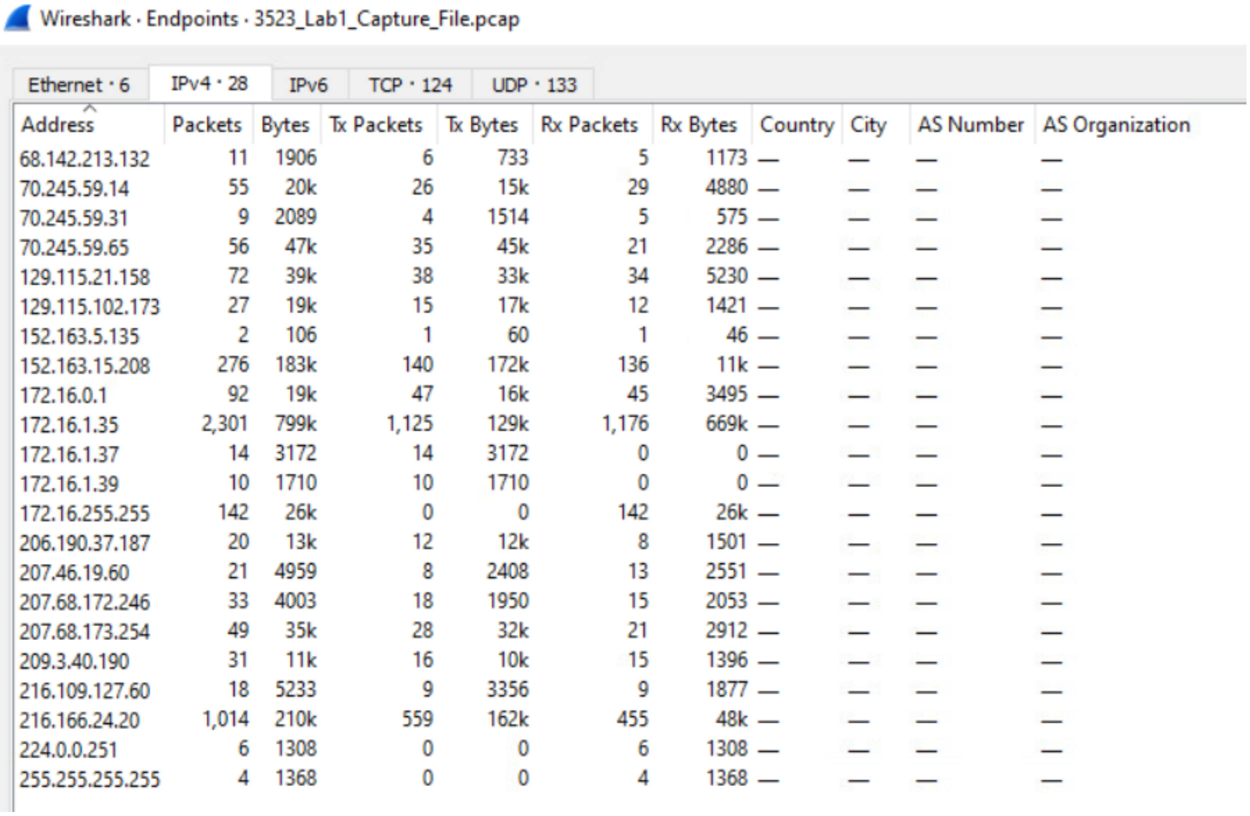
Wireshark I/O graph showing spike between 93-98 seconds.

Figure 3



Wireshark · Endpoints · 3523_Lab1_Capture_File.pcap

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	4419	12	1929	15	2490	—	—	—	—
66.39.22.157	196	40k	104	34k	92	5476	—	—	—	—
66.142.254.158	127	96k	79	92k	48	3841	—	—	—	—
66.218.70.70	17	8154	9	7118	8	1036	—	—	—	—
66.218.75.184	13	6740	7	5772	6	968	—	—	—	—
68.142.213.132	11	1906	6	733	5	1173	—	—	—	—
70.245.59.14	55	20k	26	15k	29	4880	—	—	—	—
70.245.59.31	9	2089	4	1514	5	575	—	—	—	—
70.245.59.65	56	47k	35	45k	21	2286	—	—	—	—
129.115.21.158	72	39k	38	33k	34	5230	—	—	—	—
129.115.102.173	27	19k	15	17k	12	1421	—	—	—	—
152.163.5.135	2	106	1	60	1	46	—	—	—	—
152.163.15.208	276	183k	140	172k	136	11k	—	—	—	—
172.16.0.1	92	19k	47	16k	45	3495	—	—	—	—
172.16.1.35	2,301	799k	1,125	129k	1,176	669k	—	—	—	—
172.16.1.37	14	3172	14	3172	0	0	—	—	—	—
172.16.1.39	10	1710	10	1710	0	0	—	—	—	—
172.16.255.255	142	26k	0	0	142	26k	—	—	—	—
206.190.37.187	20	13k	12	12k	8	1501	—	—	—	—
207.46.19.60	21	4959	8	2408	13	2551	—	—	—	—
207.68.172.246	33	4003	18	1950	15	2053	—	—	—	—
207.68.173.254	49	35k	28	32k	21	2912	—	—	—	—

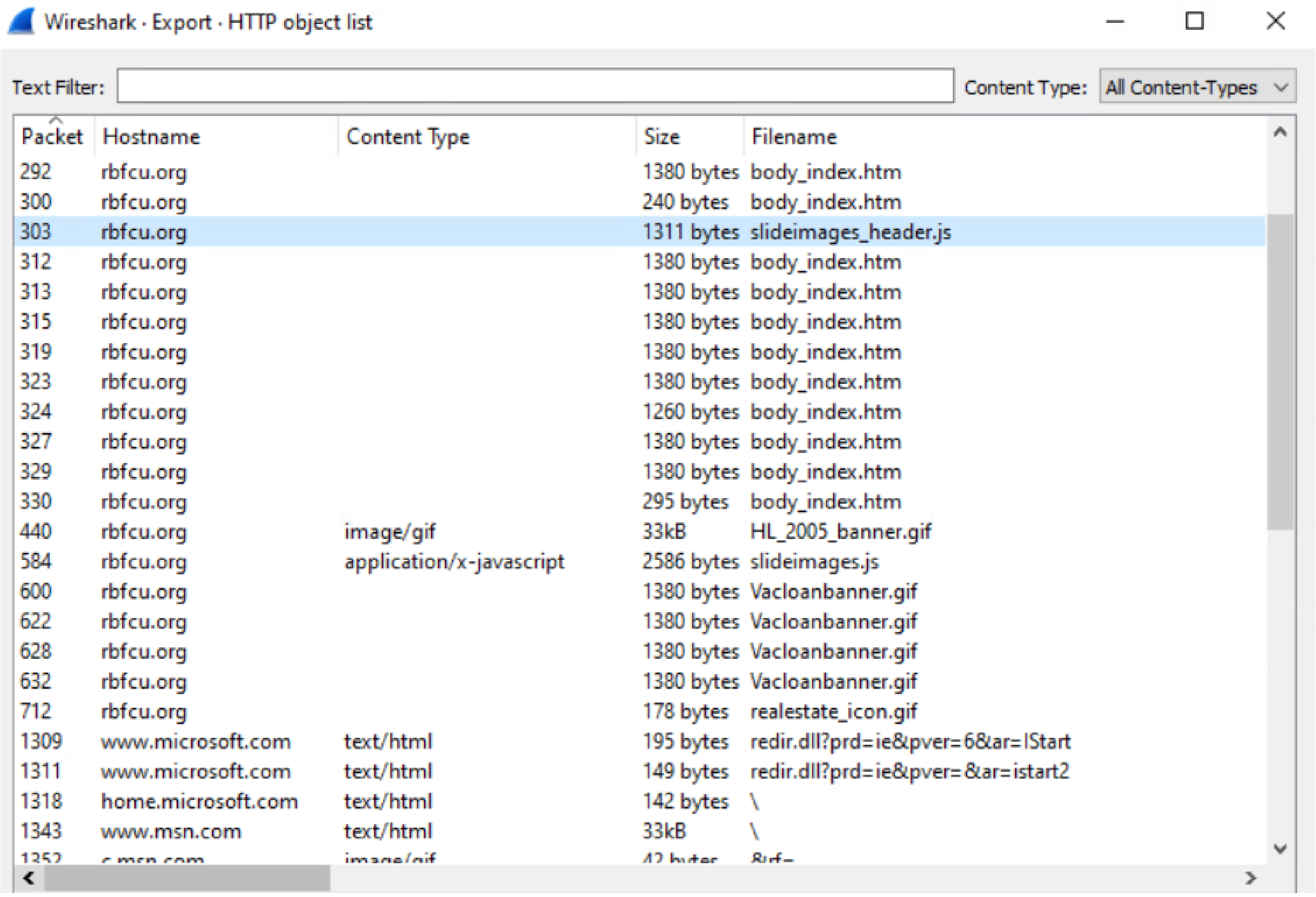


Wireshark · Endpoints · 3523_Lab1_Capture_File.pcap

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
68.142.213.132	11	1906	6	733	5	1173	—	—	—	—
70.245.59.14	55	20k	26	15k	29	4880	—	—	—	—
70.245.59.31	9	2089	4	1514	5	575	—	—	—	—
70.245.59.65	56	47k	35	45k	21	2286	—	—	—	—
129.115.21.158	72	39k	38	33k	34	5230	—	—	—	—
129.115.102.173	27	19k	15	17k	12	1421	—	—	—	—
152.163.5.135	2	106	1	60	1	46	—	—	—	—
152.163.15.208	276	183k	140	172k	136	11k	—	—	—	—
172.16.0.1	92	19k	47	16k	45	3495	—	—	—	—
172.16.1.35	2,301	799k	1,125	129k	1,176	669k	—	—	—	—
172.16.1.37	14	3172	14	3172	0	0	—	—	—	—
172.16.1.39	10	1710	10	1710	0	0	—	—	—	—
172.16.255.255	142	26k	0	0	142	26k	—	—	—	—
206.190.37.187	20	13k	12	12k	8	1501	—	—	—	—
207.46.19.60	21	4959	8	2408	13	2551	—	—	—	—
207.68.172.246	33	4003	18	1950	15	2053	—	—	—	—
207.68.173.254	49	35k	28	32k	21	2912	—	—	—	—
209.3.40.190	31	11k	16	10k	15	1396	—	—	—	—
216.109.127.60	18	5233	9	3356	9	1877	—	—	—	—
216.166.24.20	1,014	210k	559	162k	455	48k	—	—	—	—
224.0.0.251	6	1308	0	0	6	1308	—	—	—	—
255.255.255.255	4	1368	0	0	4	1368	—	—	—	—

Endpoint analysis showing connections to MSN, Yahoo, AOL, and UTSA servers.

Figure 4



Wireshark · Export · HTTP object list

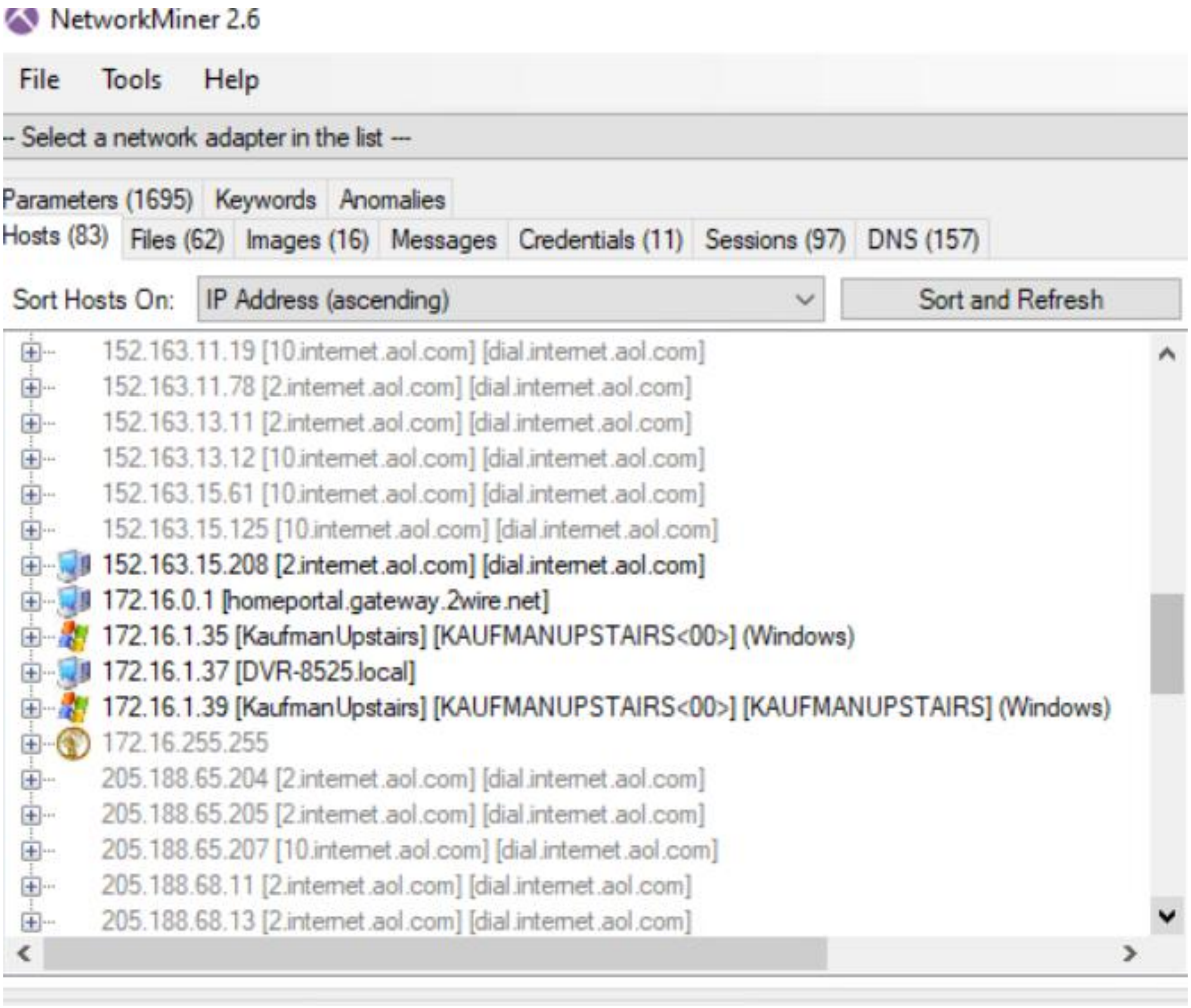
Text Filter:

Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
292	rbfcu.org		1380 bytes	body_index.htm
300	rbfcu.org		240 bytes	body_index.htm
303	rbfcu.org		1311 bytes	slideimages_header.js
312	rbfcu.org		1380 bytes	body_index.htm
313	rbfcu.org		1380 bytes	body_index.htm
315	rbfcu.org		1380 bytes	body_index.htm
319	rbfcu.org		1380 bytes	body_index.htm
323	rbfcu.org		1380 bytes	body_index.htm
324	rbfcu.org		1260 bytes	body_index.htm
327	rbfcu.org		1380 bytes	body_index.htm
329	rbfcu.org		1380 bytes	body_index.htm
330	rbfcu.org		295 bytes	body_index.htm
440	rbfcu.org	image/gif	33kB	HL_2005_banner.gif
584	rbfcu.org	application/x-javascript	2586 bytes	slideimages.js
600	rbfcu.org		1380 bytes	Vacloanbanner.gif
622	rbfcu.org		1380 bytes	Vacloanbanner.gif
628	rbfcu.org		1380 bytes	Vacloanbanner.gif
632	rbfcu.org		1380 bytes	Vacloanbanner.gif
712	rbfcu.org		178 bytes	realestate_icon.gif
1309	www.microsoft.com	text/html	195 bytes	redir.dll?prd=ie&pver=6&ar=IStart
1311	www.microsoft.com	text/html	149 bytes	redir.dll?prd=ie&pver=&ar=istart2
1318	home.microsoft.com	text/html	142 bytes	\
1343	www.msn.com	text/html	33kB	\
1352	c.msn.com	image/gif	42 bytes	&rf=

Exported HTTP object slideimages_header.js containing Javascript redirect

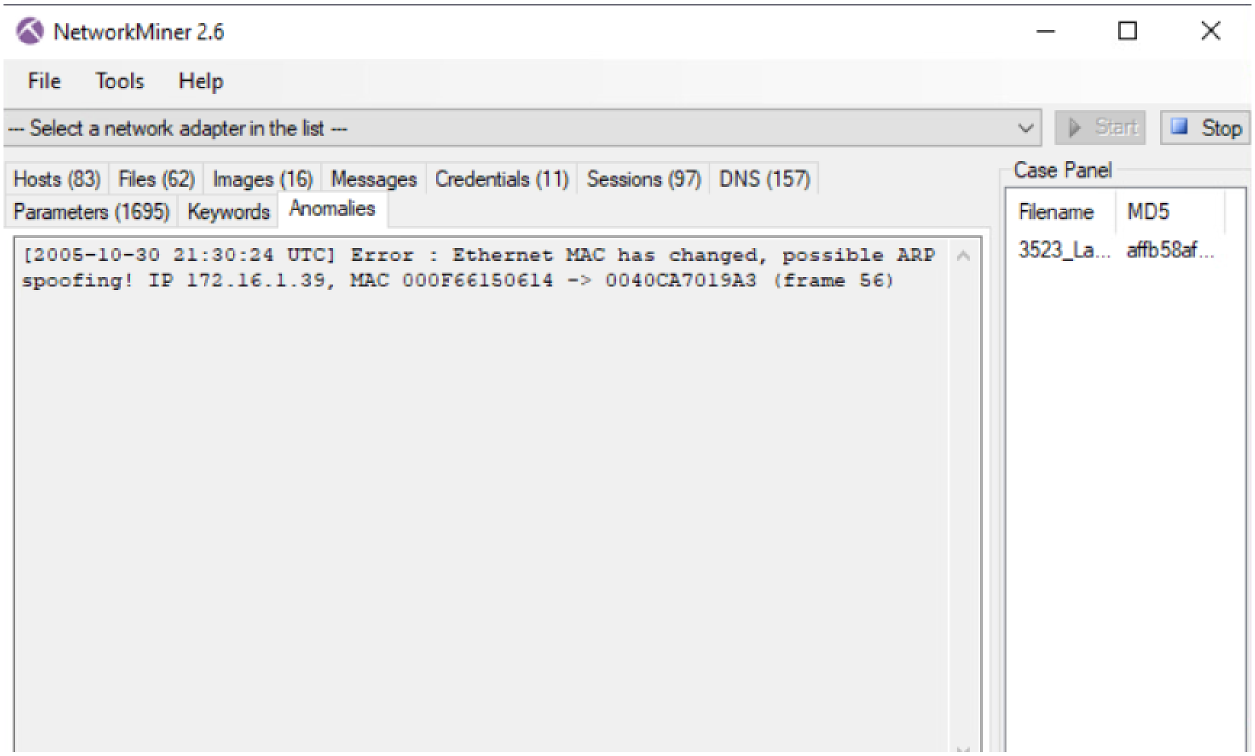
Figure 5



```
152.163.11.19 [10.internet.aol.com] [dial.internet.aol.com]
152.163.11.78 [2.internet.aol.com] [dial.internet.aol.com]
152.163.13.11 [2.internet.aol.com] [dial.internet.aol.com]
152.163.13.12 [10.internet.aol.com] [dial.internet.aol.com]
152.163.15.61 [10.internet.aol.com] [dial.internet.aol.com]
152.163.15.125 [10.internet.aol.com] [dial.internet.aol.com]
152.163.15.208 [2.internet.aol.com] [dial.internet.aol.com]
172.16.0.1 [homeportal.gateway.2wire.net]
172.16.1.35 [KaufmanUpstairs] [KAUFMANUPSTAIRS<00>] (Windows)
172.16.1.37 [DVR-8525.local]
172.16.1.39 [KaufmanUpstairs] [KAUFMANUPSTAIRS<00>] [KAUFMANUPSTAIRS] (Windows)
172.16.255.255
205.188.65.204 [2.internet.aol.com] [dial.internet.aol.com]
205.188.65.205 [2.internet.aol.com] [dial.internet.aol.com]
205.188.65.207 [10.internet.aol.com] [dial.internet.aol.com]
205.188.68.11 [2.internet.aol.com] [dial.internet.aol.com]
205.188.68.13 [2.internet.aol.com] [dial.internet.aol.com]
```

NetworkMiner host identification of KaufmanUpstairs (172.16.1.35) on Windows OS.

Figure 6

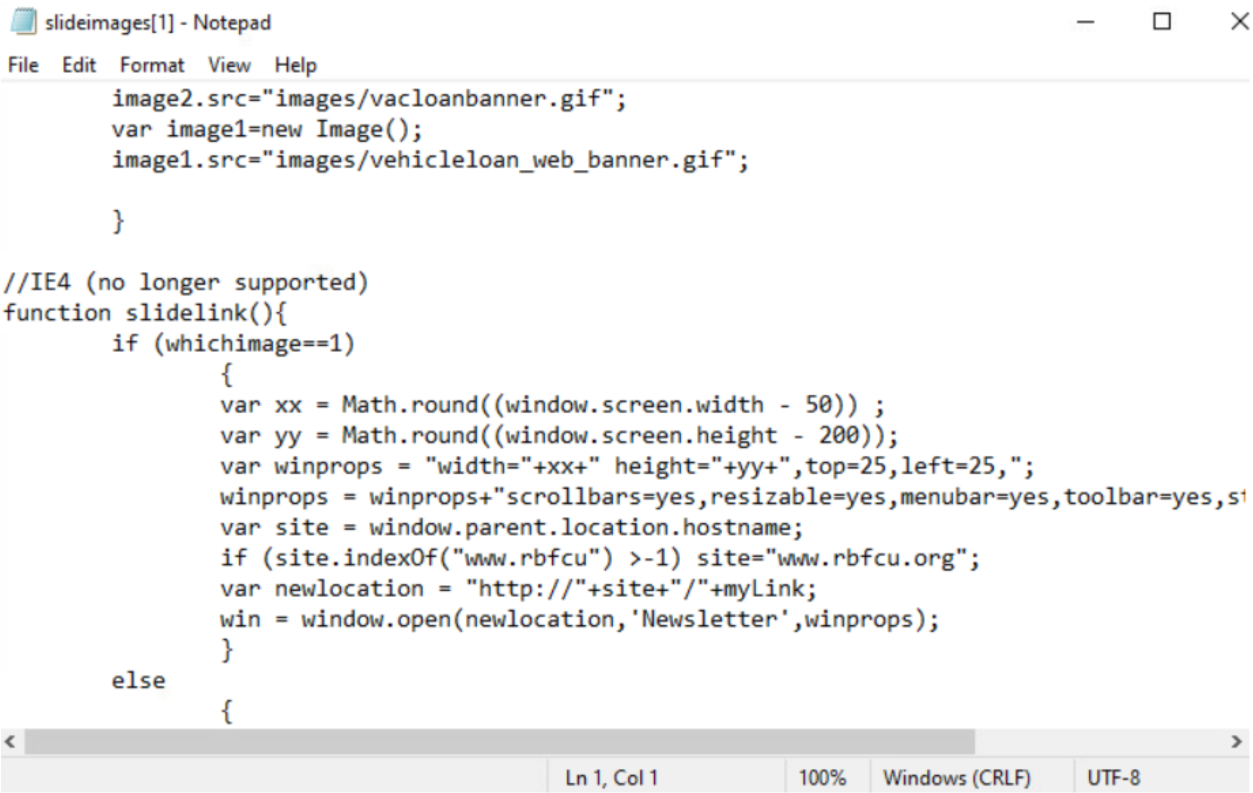


```
[2005-10-30 21:30:24 UTC] Error : Ethernet MAC has changed, possible ARP
spoofing! IP 172.16.1.39, MAC 000F66150614 -> 0040CA7019A3 (frame 56)
```

Filename	MD5
3523_La...	affb58af...

NetworkMiner anomaly showing ARP spoofing

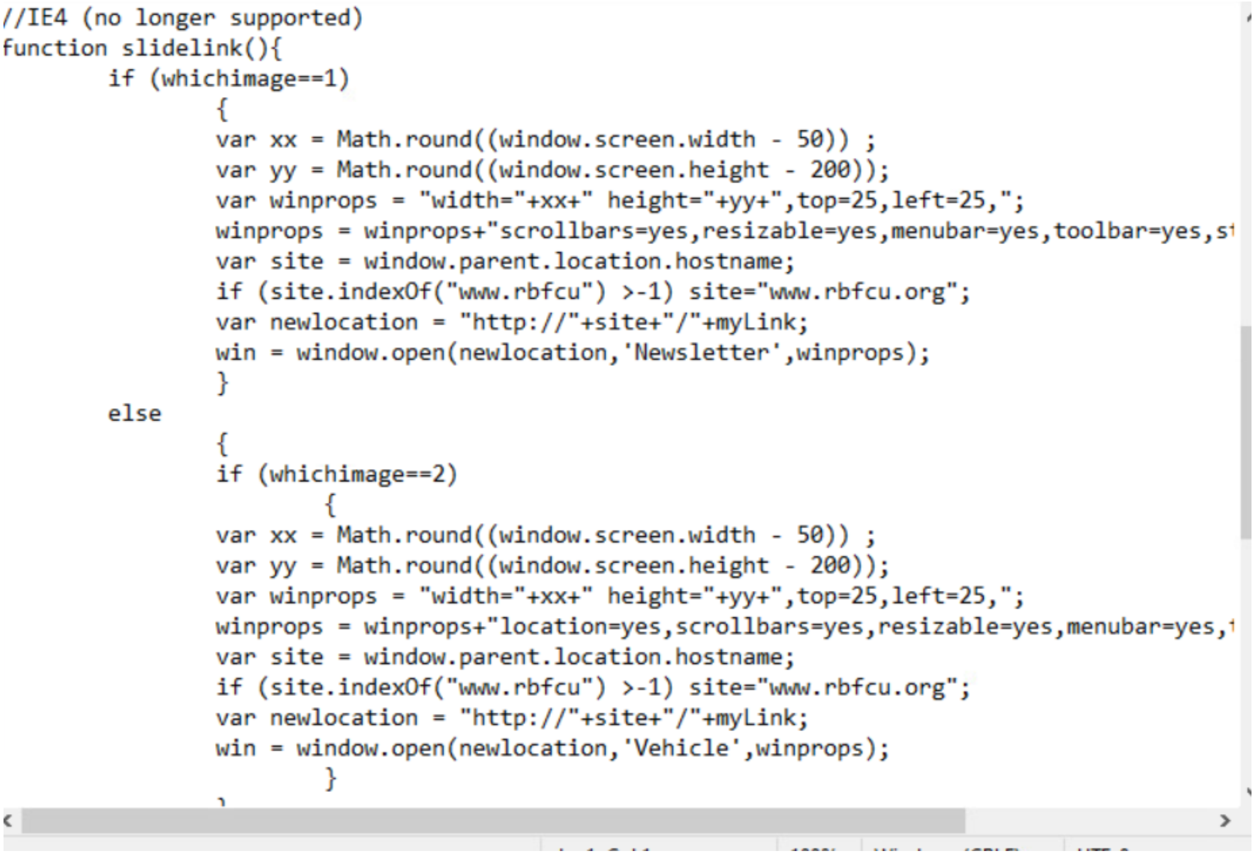
Figure 7



```
        image2.src="images/vacloanbanner.gif";
        var image1=new Image();
        image1.src="images/vehicleloan_web_banner.gif";

        }

//IE4 (no longer supported)
function slidelink(){
        if (whichimage==1)
                {
                var xx = Math.round((window.screen.width - 50)) ;
                var yy = Math.round((window.screen.height - 200));
                var winprops = "width="+xx+" height="+yy+",top=25,left=25,";
                winprops = winprops+"scrollbars=yes,resizable=yes,menubar=yes,toolbar=yes,s
                var site = window.parent.location.hostname;
                if (site.indexOf("www.rbfcu") >-1) site="www.rbfcu.org";
                var newlocation = "http://"+site+"/"+myLink;
                win = window.open(newlocation,'Newsletter',winprops);
                }
        else
                {
```



```
//IE4 (no longer supported)
function slidelink(){
        if (whichimage==1)
                {
                var xx = Math.round((window.screen.width - 50)) ;
                var yy = Math.round((window.screen.height - 200));
                var winprops = "width="+xx+" height="+yy+",top=25,left=25,";
                winprops = winprops+"scrollbars=yes,resizable=yes,menubar=yes,toolbar=yes,s
                var site = window.parent.location.hostname;
                if (site.indexOf("www.rbfcu") >-1) site="www.rbfcu.org";
                var newlocation = "http://"+site+"/"+myLink;
                win = window.open(newlocation,'Newsletter',winprops);
                }
        else
                {
                if (whichimage==2)
                        {
                var xx = Math.round((window.screen.width - 50)) ;
                var yy = Math.round((window.screen.height - 200));
                var winprops = "width="+xx+" height="+yy+",top=25,left=25,";
                winprops = winprops+"location=yes,scrollbars=yes,resizable=yes,menubar=yes,t
                var site = window.parent.location.hostname;
                if (site.indexOf("www.rbfcu") >-1) site="www.rbfcu.org";
                var newlocation = "http://"+site+"/"+myLink;
                win = window.open(newlocation,'Vehicle',winprops);
                        }
                }
```

Redirect to RBFCU fraudulent site