

# Malware Traffic Analysis using Wireshark (PCAP-Based Investigation)

## 1. Overview

Performed a network forensics investigation using Wireshark to analyze PCAP files and identify indicators of malicious activity. Applied protocol-, IP-, and flag-based display filters to isolate FTP, HTTP, DNS, and TCP traffic associated with abnormal communication patterns and potential host compromise.

## 2. Investigation Approach

Wireshark display filters were used to narrow analysis to protocol-specific and host-specific traffic within captured PCAP files. Boolean expressions and protocol fields were applied to efficiently isolate suspicious sessions and analyze communication behavior at the packet level.

## 3. Filtering Methodology

Two primary filtering approaches were used during analysis:

- **Protocol-based filtering:**
  - o Isolated traffic by protocol (DNS, FTP, HTTP, TCP)
  - o Leveraged Wireshark autocomplete and protocol-specific fields to refine analysis
- **Address- and field-based filtering:**
  - o Applied filters targeting IP addresses, ports, and protocol fields (e.g., ip.addr, tcp.port, udp.port)
  - o Used Boolean operators (&&, ||) to correlate traffic across hosts and sessions

The screenshot shows the Wireshark interface with a file named "Using-Wireshark-display-filters-FTP-malware.pcap". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations and search. A red highlight is applied to the "dns" column in the packet list, which lists several DNS-related fields such as dns.a, dns.a6.address\_suffix, dns.a6.prefix\_len, dns.a6.prefix\_name, dns.aaaa, dns.afsdb.hostname, dns.afsdb.subtype, dns.apl.address\_family, dns.apl.afdlenth, dns.apl.afdpart.data, dns.apl.afdpart.ipv4, and dns.apl.afdpart.ipv6. The main packet list displays several network packets, with the first few being DNS queries and the subsequent ones being TCP and FTP responses. The columns in the packet list are Destination, Protocol, Length, and Info.

No.	Destination	Protocol	Length	Info
1	8.8.8.8	DNS	84	Standard query 0x0
2	10.11.20.102	DNS	114	Standard query res
3	192.185.230.61	TCP	66	49158 → 21 [SYN] S
4	10.11.20.102	TCP	58	21 → 49158 [SYN, A
5	192.185.230.61	TCP	54	49158 → 21 [ACK] S
6	10.11.20.102	FTP	324	Response: 220-----
7	192.185.230.61	TCP	54	49158 → 21 [ACK] S
8	192.185.230.61	FTP	86	Request: USER schw
9	10.11.20.102	TCP	54	21 → 49158 [ACK] S
10	10.11.20.102	FTP	112	Response: 231 11<an>

Address- and field-based Wireshark display filters (IP address and protocol fields) were used to refine DNS traffic and isolate relevant network activity.

Address- and field-based display filters were used to narrow analysis to specific hosts, ports, and protocols.

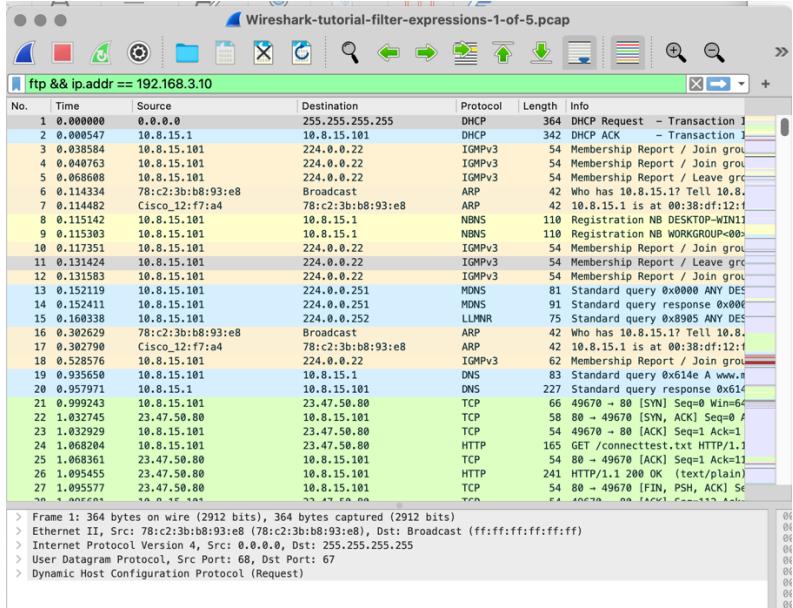
#### 4. Web-Based Traffic Analysis

Web-based traffic was analyzed to identify suspicious client behavior and repeated connection attempts indicative of potential compromise. Wireshark display filters were applied to isolate HTTP and related traffic, allowing focused inspection of request patterns and session activity.

##### - Analysis performed:

- Applied http.request display filter to isolate outbound HTTP requests initiated by the internal host.
- Filtered traffic to identify repeated connection attempts and abnormal retransmissions.
- Observed request patterns consistent with automated or non-user-initiated behavior.

The filtered results revealed active web communication between the internal host and external destinations, supporting further investigation into host behavior and potential compromise.



#### FTP Traffic Analysis

Applied the display filter `ftp && ip.addr == 192.168.3.10` to isolate FTP traffic associated with the internal host. The filter successfully returned FTP control and data packets, confirming active FTP communication involving the specified IP address.

Wireshark-tutorial-filter-expressions-1-of-5.pcap						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction 1
2	0.000547	10.8.15.1	10.8.15.101	DHCP	342	DHCP ACK - Transaction 1
3	0.038584	10.8.15.101	224.0.0.22	IGMPv3	54	Membership Report / Join group
4	0.049763	10.8.15.101	224.0.0.22	IGMPv3	54	Membership Report / Join group
5	0.068608	10.8.15.101	224.0.0.22	IGMPv3	54	Membership Report / Leave group
6	0.114334	78:c2:3b:08:93:e8	Broadcast	ARP	42	Who has 10.8.15.1? Tell 10.8.
7	0.114482	Cisco_12:ff:a4	78:c2:3b:08:93:e8	ARP	42	10.8.15.1 is at 00:38:df:12:f
8	0.115142	10.8.15.101	10.8.15.1	NBNS	110	Registration NB DESKTOP-WIN11
9	0.115503	10.8.15.101	10.8.15.1	NBNS	110	Registration NB WORKGROUP<0>
10	0.117731	10.8.15.101	224.0.0.22	IGMPv3	54	Membership Report / Join group
11	0.131424	10.8.15.101	224.0.0.22	IGMPv3	54	Membership Report / Leave group
12	0.131583	10.8.15.101	224.0.0.22	IGMPv3	54	Membership Report / Join group
13	0.152119	10.8.15.101	224.0.0.251	MDNS	81	Standard query 0x0000 ANY DES
14	0.152411	10.8.15.101	224.0.0.251	MDNS	91	Standard query response 0x0000
15	0.160338	10.8.15.101	224.0.0.252	LLMNR	75	Standard query 0x8905 ANY DES
16	0.302629	78:c2:3b:08:93:e8	Broadcast	ARP	42	Who has 10.8.15.1? Tell 10.8.
17	0.302790	Cisco_12:ff:a4	78:c2:3b:08:93:e8	ARP	42	10.8.15.1 is at 00:38:df:12:f
18	0.528576	10.8.15.101	224.0.0.22	IGMPv3	62	Membership Report / Join group
19	0.935650	10.8.15.101	10.8.15.1	DNS	83	Standard query 0x614 A www.ill
20	0.957971	10.8.15.101	10.8.15.101	DNS	227	Standard query response 0x614
21	0.999243	10.8.15.101	23.47.50.80	TCP	66	49670 -> 80 [SYN] Seq=0 Win=64
22	1.032745	23.47.50.80	10.8.15.101	TCP	58	80 -> 49670 [SYN, ACK] Seq=0 /
23	1.032929	10.8.15.101	23.47.50.80	TCP	54	49670 -> 80 [ACK] Seq=1 Ack=1
24	1.068284	10.8.15.101	23.47.50.80	HTTP	165	GET /connecttest.txt HTTP/1.1
25	1.068361	23.47.50.80	10.8.15.101	TCP	54	80 -> 49670 [ACK] Seq=1 Ack=1
26	1.095455	23.47.50.80	10.8.15.101	HTTP	241	HTTP/1.1 200 OK (text/plain)
27	1.095577	23.47.50.80	10.8.15.101	TCP	54	80 -> 49670 [FIN, PSH, ACK] Seq=112 Ack=113

> Frame 1: 364 bytes on wire (2912 bits), 364 bytes captured (2912 bits)  
 > Ethernet II, Src: 78:c2:3b:08:93:e8 (78:c2:3b:08:93:e8), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
 > Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255  
 > User Datagram Protocol, Src Port: 68, Dst Port: 67  
 > Dynamic Host Configuration Protocol (Request)

## HTTP Traffic Analysis

Applied the display filter http.request || http.response to isolate inbound and outbound HTTP communication. The filtered results revealed active HTTP sessions between the internal host and external servers, confirming normal request-response behavior and enabling further session-level inspection.

Wireshark-tutorial-filter-expressions-1-of-5.pcap						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction 1
2	0.000547	10.8.15.1	10.8.15.101	DHCP	342	DHCP ACK - Transaction 1
3	0.038584	10.8.15.101	224.0.0.22	IGMPv3	54	Membership Report / Join group
4	0.049763	10.8.15.101	224.0.0.22	IGMPv3	54	Membership Report / Join group
5	0.068608	10.8.15.101	224.0.0.22	IGMPv3	54	Membership Report / Leave group
6	0.114334	78:c2:3b:08:93:e8	Broadcast	ARP	42	Who has 10.8.15.1? Tell 10.8.
7	0.114482	Cisco_12:ff:a4	78:c2:3b:08:93:e8	ARP	42	10.8.15.1 is at 00:38:df:12:f
8	0.115142	10.8.15.101	10.8.15.1	NBNS	110	Registration NB DESKTOP-WIN11
9	0.115503	10.8.15.101	10.8.15.1	NBNS	110	Registration NB WORKGROUP<0>
10	0.117731	10.8.15.101	224.0.0.22	IGMPv3	54	Membership Report / Join group
11	0.131424	10.8.15.101	224.0.0.22	IGMPv3	54	Membership Report / Leave group
12	0.131583	10.8.15.101	224.0.0.22	IGMPv3	54	Membership Report / Join group
13	0.152119	10.8.15.101	224.0.0.251	MDNS	81	Standard query 0x0000 ANY DES
14	0.152411	10.8.15.101	224.0.0.251	MDNS	91	Standard query response 0x0000
15	0.160338	10.8.15.101	224.0.0.252	LLMNR	75	Standard query 0x8905 ANY DES
16	0.302629	78:c2:3b:08:93:e8	Broadcast	ARP	42	Who has 10.8.15.1? Tell 10.8.
17	0.302790	Cisco_12:ff:a4	78:c2:3b:08:93:e8	ARP	42	10.8.15.1 is at 00:38:df:12:f
18	0.528576	10.8.15.101	224.0.0.22	IGMPv3	62	Membership Report / Join group
19	0.935650	10.8.15.101	10.8.15.1	DNS	83	Standard query 0x614 A www.ill
20	0.957971	10.8.15.101	10.8.15.101	DNS	227	Standard query response 0x614
21	0.999243	10.8.15.101	23.47.50.80	TCP	66	49670 -> 80 [SYN] Seq=0 Win=64
22	1.032745	23.47.50.80	10.8.15.101	TCP	58	80 -> 49670 [SYN, ACK] Seq=0 /
23	1.032929	10.8.15.101	23.47.50.80	TCP	54	49670 -> 80 [ACK] Seq=1 Ack=1
24	1.068284	10.8.15.101	23.47.50.80	HTTP	165	GET /connecttest.txt HTTP/1.1
25	1.068361	23.47.50.80	10.8.15.101	TCP	54	80 -> 49670 [ACK] Seq=1 Ack=11
26	1.095455	23.47.50.80	10.8.15.101	HTTP	241	HTTP/1.1 200 OK (text/plain)
27	1.095577	23.47.50.80	10.8.15.101	TCP	54	80 -> 49670 [FIN, PSH, ACK] Seq=112 Ack=113

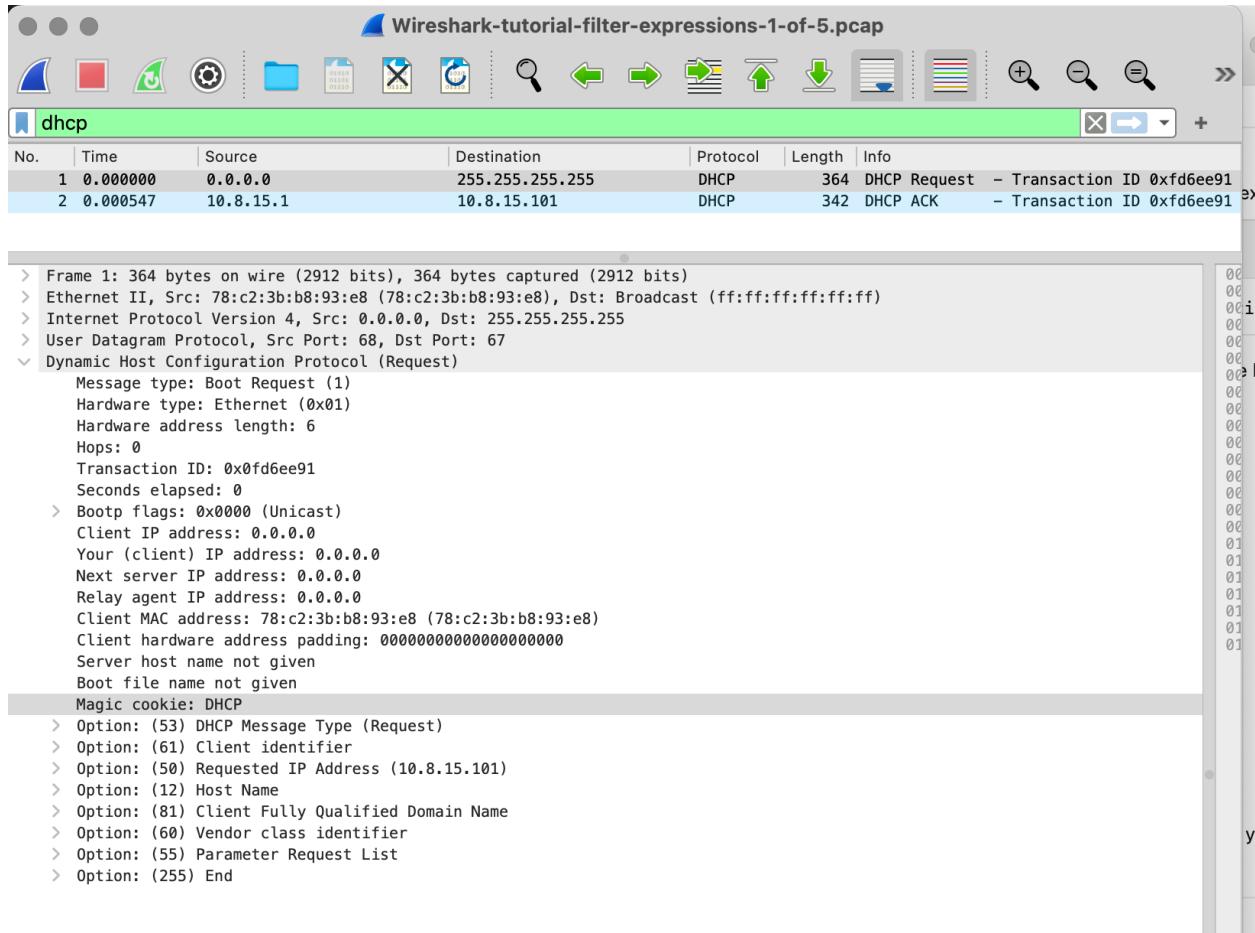
> Frame 1: 364 bytes on wire (2912 bits), 364 bytes captured (2912 bits)  
 > Ethernet II, Src: 78:c2:3b:08:93:e8 (78:c2:3b:08:93:e8), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
 > Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255  
 > User Datagram Protocol, Src Port: 68, Dst Port: 67  
 > Dynamic Host Configuration Protocol (Request)

## DNS Traffic Analysis

Applied the display filter dns.qry.name contains "apple" to identify DNS queries associated with Apple-related domains. The results confirmed external name resolution activity and helped establish baseline DNS behavior for the host.

## 5. Identifying Hosts and Users

### Step 3: Host name and MAC address

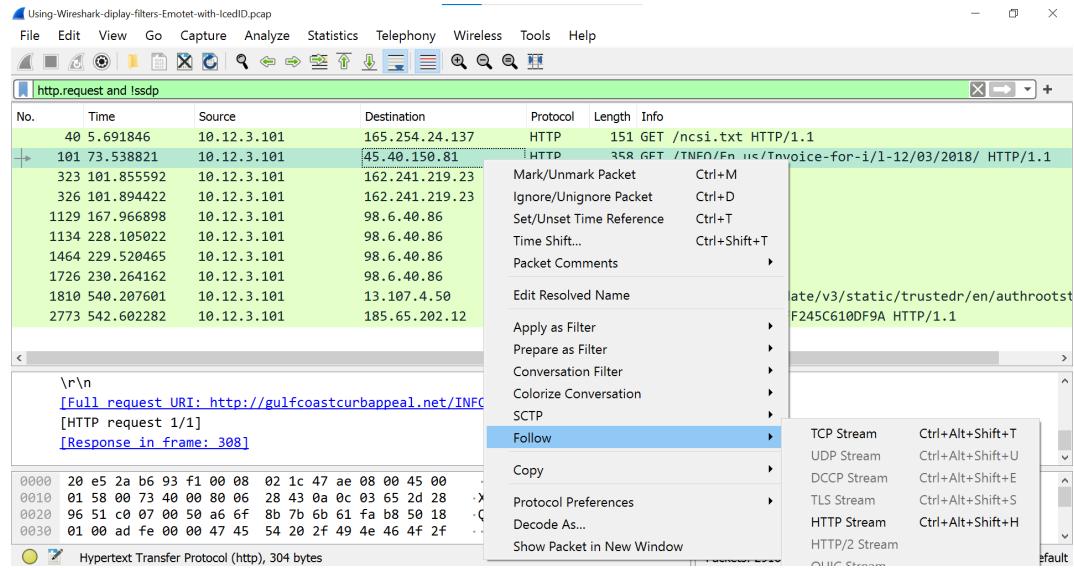


### Host Identification via DHCP

DHCP traffic was analyzed to identify the internal host responsible for initiating network activity. Inspection of the DHCP Request packet revealed the client MAC address **78:c2:3b:b8:93:e8**, which was used to associate subsequent traffic with a specific device. No hostname was included in the DHCP options, indicating the host did not advertise a hostname during the request.

## 6. Operating System

User-agent strings from headers in HTTP traffic can reveal the operating system. If the HTTP traffic is from an Android device, you might also determine the manufacturer and model of the device.



### Operating System Identification

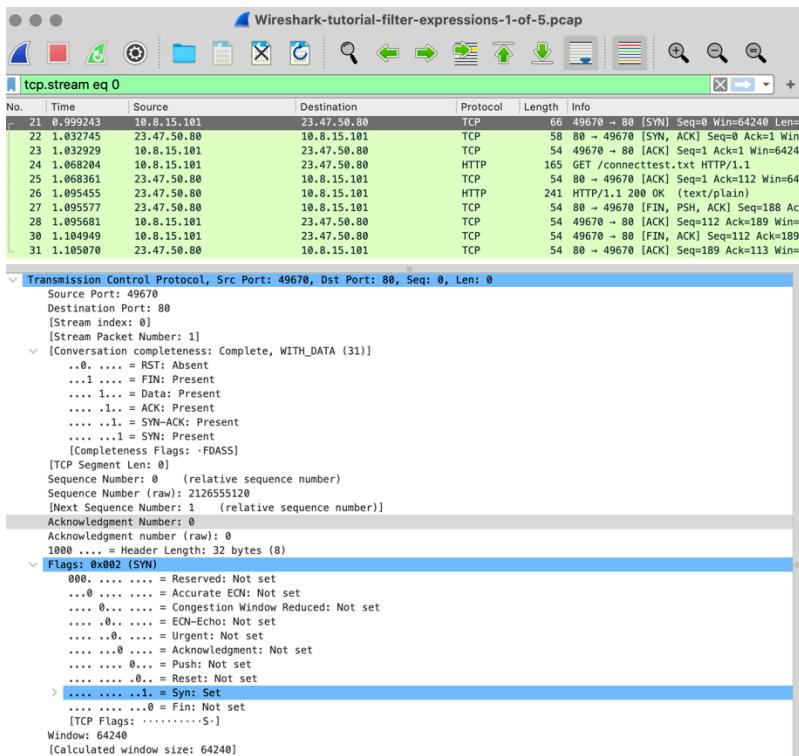
HTTP traffic was analyzed to determine the operating system of the infected host by inspecting the User-Agent header within HTTP requests. The display filter http.request and !(ssdp) was applied to isolate relevant HTTP traffic.

Inspection of the TCP stream associated with destination IP address **23.47.50.80** revealed the following User-Agent string:

User-Agent: Microsoft NCSI

This User-Agent indicates that the host is running a Microsoft Windows operating system, as Microsoft NCSI (Network Connectivity Status Indicator) is used by Windows systems to perform connectivity checks.

Additionally, analysis of the TCP three-way handshake between **10.8.15.101** and **23.47.50.80** confirmed a successful TCP connection establishment, supporting normal HTTP communication behavior between the internal host and the external server.



The following screenshots provide supporting packet-level evidence for the operating system identification and TCP connection establishment discussed in Step 4.

Wireshark-tutorial-filter-expressions-1-of-5.pcap

tcp.stream eq 0

No.	Time	Source	Destination	Protocol	Length	Info
21	0.999243	10.8.15.101	23.47.50.80	TCP	66	49670 → 80 [SYN] Seq=0 Win=64240 Len=0
22	1.032745	23.47.50.80	10.8.15.101	TCP	58	80 → 49670 [SYN, ACK] Seq=0 Ack=1 Win=64240
23	1.032929	10.8.15.101	23.47.50.80	TCP	54	49670 → 80 [ACK] Seq=1 Ack=1 Win=64240
24	1.066284	10.8.15.101	23.47.50.80	HTTP	165	GET /connecttest.txt HTTP/1.1
25	1.066361	23.47.50.80	10.8.15.101	TCP	54	80 → 49670 [ACK] Seq=12 Ack=12 Win=64240
26	1.095455	23.47.50.80	10.8.15.101	HTTP	241	HTTP/1.1 200 OK (text/plain)
27	1.095577	23.47.50.80	10.8.15.101	TCP	54	80 → 49670 [FIN, PSH, ACK] Seq=188 Ack=189 Win=64240
28	1.095681	10.8.15.101	23.47.50.80	TCP	54	49670 → 80 [ACK] Seq=112 Ack=189 Win=64240
30	1.104949	10.8.15.101	23.47.50.80	TCP	54	49670 → 80 [FIN, ACK] Seq=112 Ack=189 Win=64240
31	1.105070	23.47.50.80	10.8.15.101	TCP	54	80 → 49670 [ACK] Seq=189 Ack=113 Win=64240

Destination Port: 49670  
[Stream index: 0]  
[Stream Packet Number: 2]  
[Conversation completeness: Complete, WITH\_DATA (31)]  
...0.... = RST: Absent  
...1.... = FIN: Present  
....1.... = Data: Present  
....1.. = ACK: Present  
....1.. = SYN-ACK: Present  
....1.. = SYN: Present  
[Completeness Flags: FDASS]  
[TCP Segment Len: 0]  
Sequence Number: 0 (relative sequence number)  
Sequence Number (raw): 1945379785  
[Next Sequence Number: 1 (relative sequence number)]  
Acknowledgment Number: 1 (relative ack number)  
Acknowledgment number (raw): 2126555121  
0101.... = Header Length: 24 bytes (6)  
Flags: 0x012 (SYN, ACK)  
000.... = Reserved: Not set  
...0.... = Accurate ECN: Not set  
...0.... = Congestion Window Reduced: Not set  
...0.... = ECN-Echo: Not set  
....0.... = Urgent: Not set  
....1.... = Acknowledgment: Set  
....0.... = Push: Not set  
....0.... = Reset: Not set  
> ....0.... = Syn: Set  
....0.... = Fin: Not set  
[TCP Flags: .....A-S-]  
Window: 64240  
[Calculated window size: 64240]  
Checksum: 0xb973 [unverified]  
[Checksum Status: Unverified]  
Urgent Pointer: 0  
Options: (4 bytes), Maximum segment size  
[Timestamps]  
[Time since first frame in this TCP stream: 0.033502000 seconds]  
[Time since previous frame in this TCP stream: 0.033502000 seconds]  
[SEQ/ACK analysis]

Wireshark-tutorial-filter-expressions-1-of-5.pcap

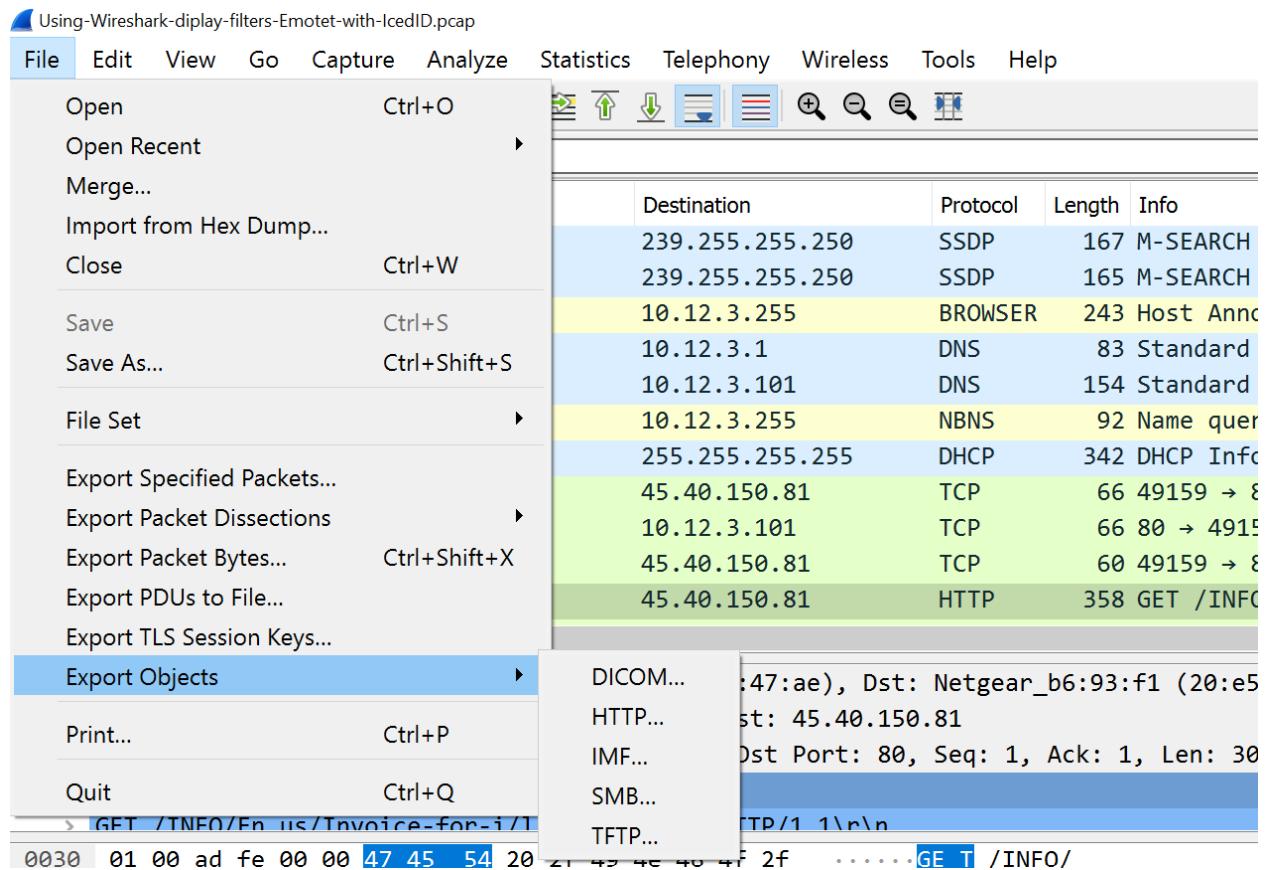
tcp.stream eq 0

No.	Time	Source	Destination	Protocol	Length	Info
21	0.999243	10.8.15.101	23.47.50.80	TCP	66	49670 → 80 [SYN] Seq=0 Win=64240 Len=0
22	1.032745	23.47.50.80	10.8.15.101	TCP	58	80 → 49670 [SYN, ACK] Seq=0 Ack=1 Win=64240
23	1.032929	10.8.15.101	23.47.50.80	TCP	54	49670 → 80 [ACK] Seq=1 Ack=1 Win=64240 L
24	1.066284	10.8.15.101	23.47.50.80	HTTP	165	GET /connecttest.txt HTTP/1.1
25	1.066361	23.47.50.80	10.8.15.101	TCP	54	80 → 49670 [ACK] Seq=1 Ack=12 Win=64240
26	1.095455	23.47.50.80	10.8.15.101	HTTP	241	HTTP/1.1 200 OK (text/plain)
27	1.095577	23.47.50.80	10.8.15.101	TCP	54	80 → 49670 [FIN, PSH, ACK] Seq=188 Ack=189 Win=64240
28	1.095681	10.8.15.101	23.47.50.80	TCP	54	49670 → 80 [ACK] Seq=112 Ack=189 Win=64240
30	1.104949	10.8.15.101	23.47.50.80	TCP	54	49670 → 80 [FIN, ACK] Seq=112 Ack=189 Win=64240
31	1.105070	23.47.50.80	10.8.15.101	TCP	54	80 → 49670 [ACK] Seq=189 Ack=113 Win=64240

Destination Port: 80  
[Stream index: 0]  
[Stream Packet Number: 2]  
[Conversation completeness: Complete, WITH\_DATA (31)]  
...0.... = RST: Absent  
...1.... = FIN: Present  
....1.... = Data: Present  
....1.. = ACK: Present  
....1.. = SYN-ACK: Present  
....1.. = SYN: Present  
[Completeness Flags: -FDASS]  
[TCP Segment Len: 0]  
Sequence Number: 1 (relative sequence number)  
Sequence Number (raw): 2126555121  
[Next Sequence Number: 1 (relative sequence number)]  
Acknowledgment Number: 1 (relative ack number)  
Acknowledgment number (raw): 1945379786  
0101.... = Header Length: 20 bytes (5)  
Flags: 0x010 (ACK)  
000.... = Reserved: Not set  
...0.... = Accurate ECN: Not set  
...0.... = Congestion Window Reduced: Not set  
...0.... = ECN-Echo: Not set  
....0.... = Urgent: Not set  
....1.... = Acknowledgment: Set  
....0.... = Push: Not set  
....0.... = Reset: Not set  
....0.... = Sync: Not set  
....0.... = Fin: Not set  
[TCP Flags: .....A-...]  
Window: 64240  
[Calculated window size: 64240]  
[Window size scaling factor: -2 (no window scaling used)]  
Checksum: 0xd130 [unverified]  
[Checksum Status: Unverified]  
Urgent Pointer: 0  
[Timestamps]  
[Time since first frame in this TCP stream: 0.033686000 seconds]  
[Time since previous frame in this TCP stream: 0.000184000 seconds]  
[SEQ/ACK analysis]

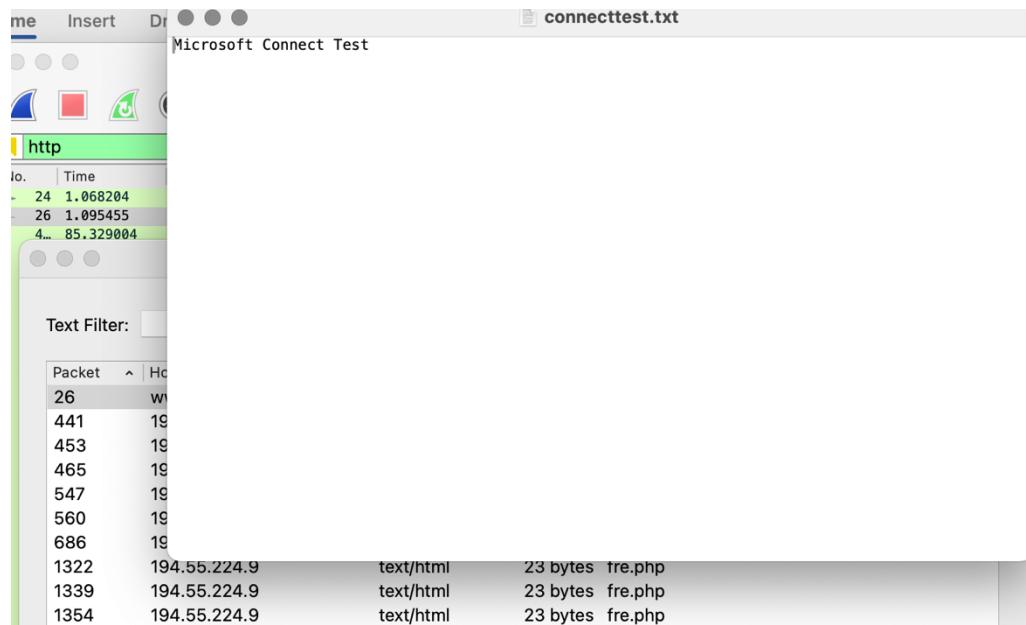
**7. CP Stream and Handshake Evidence:** The screenshots above show the TCP stream and associated flags exchanged between the internal host and the external destination, confirming successful session establishment prior to HTTP data transfer.

## 8. Export objects from HTTP traffic



## 9. Extracted File Analysis:

The extracted file, connecttest.txt, contains content associated with Microsoft Network Connectivity Status Indicator (NCSI) checks. This confirms normal Windows connectivity behavior and aligns with the previously identified User-Agent information.



## 10. Extracted File Preview