NETWORK FORENSIC REPORT

IA473 – ASSIGNMENT THREE

Jesse Russell

10/13/21

EXECUTIVE SUMMARY:

In this packet capture, two PCs on a network are communicating using a popular peer-to-peer sharing protocol, BitTorrent. This protocol is typically used to transmit larger files that may not arrive successfully using other transport protocols. To begin the transmission, the recipient PC first sends a handshake request to the PC with the needed files, which is then acknowledged by that PC. Once the handshake is complete, the recipient PC asks if the sender PC has the required pieces to build the files. Then, the sender PC sends a message including which pieces it has. The recipient PC then tell the sender that it's interested in these pieces, and the sender transmits them. Because the protocol uses TCP and sequences the pieces to be put back together later, it ensures delivery and reduces bandwidth used at one specific time. This makes it an effective tool for filesharing. Often, BitTorrent is associated with digital piracy, as the methodology used for transmission allows for a greater sense of anonymity. However, BitTorrent is commonly used for innocent file sharing between two points of communication, so the presence of this protocol is not substantial evidence to claim these users are using it for any malice.

NETWORK CAPTURE FILE DETAILS

Capture Length: 43kb

Packet Size: 65535 bytes

First Packet: 2007-04-11 12:51:36

Last Packet: 2007-04-11 12:51:45

Elapsed Time: 00:08 (0 minutes and 8 seconds)

Computed Hashes of IA473-BITTORRENT-CAPTURE.pcap:

MD5: 142d80fe1acfe7e88bffe4797a1414d2

SHA1: f8d053fa97e256edf136709c1bc92e05585a6ea2

Network Components Identified:

Hostname	IP Address	MAC Address
Microsof_3e:d0:dc	10.10.10.22	(00:03:ff:3e:d0:dc)
Microsof_3f:d0:dc	10.10.10.23	(00:03:ff:3f:d0:dc)

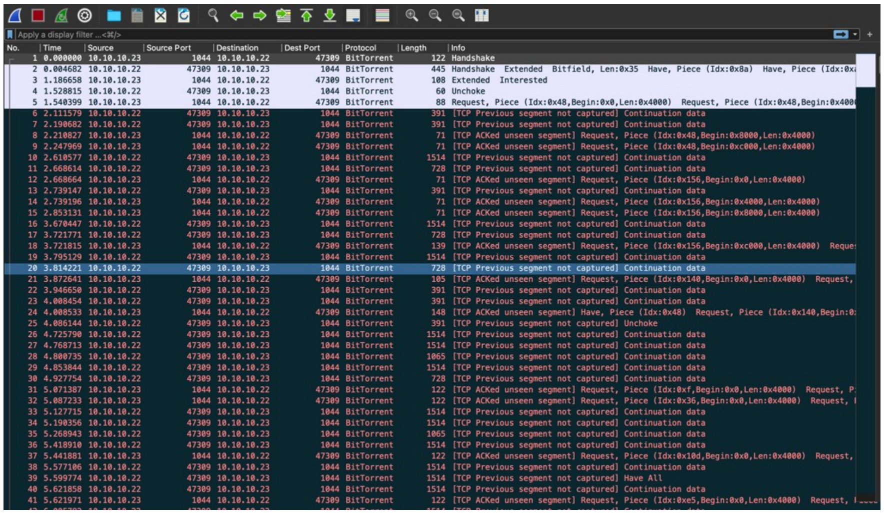
Methodology:

The packet analysis of IA473-BITTORRENT-CAPTURE.pcap was done using the industry standard packet analysis program, Wireshark (Version 3.49). Wireshark was run on an Apple MacBook Pro with the Apple Silicon M1 ARM chip, 16 GB of RAM, 256 GB of storage, and running MacOS Big Sur 11.6. Due to this Mac version of Wireshark being built on Intel's x86-x64 architecture, the M1 machine runs the program over a translation layer, called Rosetta 2. This layer should not affect any forensic results but is included here to specify any variables that may result in a different conclusion. In order to calculate the SHA-1 hash, Wireshark's built-in hash calculator was used. This was found by looking at the capture's properties. Wireshark does not natively calculate MD5, however, so this was calculated using the MD5 calculator from the terminal of MacOS.

The command used to calculate the MD5 hash: ʹmd5 <directory path> /IA473–BITTORRENT–CAPTURE.pcapʹ

Findings:

- 10.10.10.23 sends a handshake request to 10.10.10.22.
- 10.10.10.22 returns an acknowledgement of the handshake and lists the pieces that it has.
- 10.10.10.23 acknowledges the pieces available and sends a message telling 10.10.10.22 that it's interested in receiving those pieces.
- 10.10.10.22 acknowledges the interested message and unchokes 10.10.10.23, which allows the data to be sent over the wire.
- 10.10.10.23 sends a request for those pieces, beginning the transfer of the file(s).
- This process is repeated for the rest of the capture, but Wireshark did not capture all of it, just that it was being transmitted. Only the first 5 packets out of 53 are completely accounted for by Wireshark, as you can see in the screenshot below.



No.	Time	Source	Source Port	Destination	Dest Port	Protocol	Length	Info
1	0.000000	10.10.10.23	1044	10.10.10.22	47309	BitTorrent	122	Handshake
2	0.004682	10.10.10.22	47309	10.10.10.23	1044	BitTorrent	445	Handshake Extended Bitfield, Len:0x35 Have, Piece (Idx:0x8a) Have, Piece (Idx:0x
3	1.186658	10.10.10.23	1044	10.10.10.22	47309	BitTorrent	108	Extended Interested
4	1.528815	10.10.10.22	47309	10.10.10.23	1044	BitTorrent	60	Unchoke
5	1.540399	10.10.10.23	1044	10.10.10.22	47309	BitTorrent	88	Request, Piece (Idx:0x48,Begin:0x0,Len:0x4000) Request, Piece (Idx:0x48,Begin:0x400
6	2.111579	10.10.10.22	47309	10.10.10.23	1044	BitTorrent	391	[TCP Previous segment not captured] Continuation data
7	2.190682	10.10.10.22	47309	10.10.10.23	1044	BitTorrent	391	[TCP Previous segment not captured] Continuation data
8	2.210827	10.10.10.23	1044	10.10.10.22	47309	BitTorrent	71	[TCP ACKed unseen segment] Request, Piece (Idx:0x48,Begin:0x8000,Len:0x4000)
9	2.247969	10.10.10.23	1044	10.10.10.22	47309	BitTorrent	71	[TCP ACKed unseen segment] Request, Piece (Idx:0x48,Begin:0xc000,Len:0x4000)
10	2.610577	10.10.10.22	47309	10.10.10.23	1044	BitTorrent	1514	[TCP Previous segment not captured] Continuation data
11	2.668614	10.10.10.22	47309	10.10.10.23	1044	BitTorrent	728	[TCP Previous segment not captured] Continuation data
12	2.668664	10.10.10.23	1044	10.10.10.22	47309	BitTorrent	71	[TCP ACKed unseen segment] Request, Piece (Idx:0x156,Begin:0x0,Len:0x4000)
13	2.739147	10.10.10.22	47309	10.10.10.23	1044	BitTorrent	391	[TCP Previous segment not captured] Continuation data
14	2.739196	10.10.10.23	1044	10.10.10.22	47309	BitTorrent	71	[TCP ACKed unseen segment] Request, Piece (Idx:0x156,Begin:0x4000,Len:0x4000)
15	2.853131	10.10.10.23	1044	10.10.10.22	47309	BitTorrent	71	[TCP ACKed unseen segment] Request, Piece (Idx:0x156,Begin:0x8000,Len:0x4000)
16	3.670447	10.10.10.22	47309	10.10.10.23	1044	BitTorrent	1514	[TCP Previous segment not captured] Continuation data
17	3.721771	10.10.10.22	47309	10.10.10.23	1044	BitTorrent	728	[TCP Previous segment not captured] Continuation data
18	3.721815	10.10.10.23	1044	10.10.10.22	47309	BitTorrent	139	[TCP ACKed unseen segment] Request, Piece (Idx:0x156,Begin:0xc000,Len:0x4000) Reque
19	3.795129	10.10.10.22	47309	10.10.10.23	1044	BitTorrent	1514	[TCP Previous segment not captured] Continuation data
20	3.814221	10.10.10.22	47309	10.10.10.23	1044	BitTorrent	728	[TCP Previous segment not captured] Continuation data
21	3.872641	10.10.10.23	1044	10.10.10.22	47309	BitTorrent	105	[TCP ACKed unseen segment] Request, Piece (Idx:0x140,Begin:0x0,Len:0x4000) Request,
22	3.946650	10.10.10.22	47309	10.10.10.23	1044	BitTorrent	391	[TCP Previous segment not captured] Continuation data
23	4.008454	10.10.10.22	47309	10.10.10.23	1044	BitTorrent	391	[TCP Previous segment not captured] Continuation data
24	4.008533	10.10.10.23	1044	10.10.10.22	47309	BitTorrent	148	[TCP ACKed unseen segment] Have, Piece (Idx:0x48) Request, Piece (Idx:0x140,Begin:0
25	4.086144	10.10.10.22	47309	10.10.10.23	1044	BitTorrent	391	[TCP Previous segment not captured] Unchoke
26	4.725790	10.10.10.22	47309	10.10.10.23	1044	BitTorrent	1514	[TCP Previous segment not captured] Continuation data
27	4.768713	10.10.10.22	47309	10.10.10.23	1044	BitTorrent	1514	[TCP Previous segment not captured] Continuation data
28	4.800735	10.10.10.22	47309	10.10.10.23	1044	BitTorrent	1065	[TCP Previous segment not captured] Continuation data
29	4.853844	10.10.10.22	47309	10.10.10.23	1044	BitTorrent	1514	[TCP Previous segment not captured] Continuation data
30	4.927754	10.10.10.22	47309	10.10.10.23	1044	BitTorrent	728	[TCP Previous segment not captured] Continuation data
31	5.071387	10.10.10.23	1044	10.10.10.22	47309	BitTorrent	122	[TCP ACKed unseen segment] Request, Piece (Idx:0xf,Begin:0x0,Len:0x4000) Request, P
32	5.087233	10.10.10.23	1044	10.10.10.22	47309	BitTorrent	122	[TCP ACKed unseen segment] Request, Piece (Idx:0x36,Begin:0x0,Len:0x4000) Request,
33	5.127715	10.10.10.22	47309	10.10.10.23	1044	BitTorrent	1514	[TCP Previous segment not captured] Continuation data
34	5.190356	10.10.10.22	47309	10.10.10.23	1044	BitTorrent	1514	[TCP Previous segment not captured] Continuation data
35	5.268943	10.10.10.22	47309	10.10.10.23	1044	BitTorrent	1065	[TCP Previous segment not captured] Continuation data
36	5.418910	10.10.10.22	47309	10.10.10.23	1044	BitTorrent	1514	[TCP Previous segment not captured] Continuation data
37	5.441881	10.10.10.23	1044	10.10.10.22	47309	BitTorrent	122	[TCP ACKed unseen segment] Request, Piece (Idx:0x10d,Begin:0x0,Len:0x4000) Request,
38	5.577106	10.10.10.22	47309	10.10.10.23	1044	BitTorrent	1514	[TCP Previous segment not captured] Continuation data
39	5.599774	10.10.10.22	47309	10.10.10.23	1044	BitTorrent	1514	[TCP Previous segment not captured] Have All
40	5.621858	10.10.10.22	47309	10.10.10.23	1044	BitTorrent	1514	[TCP Previous segment not captured] Continuation data
41	5.621971	10.10.10.23	1044	10.10.10.22	47309	BitTorrent	122	[TCP ACKed unseen segment] Request, Piece (Idx:0xe5,Begin:0x0,Len:0x4000) Request,

- The conversations dialogue shows that 10.10.10.22 sent 36 packets to 10.10.10.23 and 10.10.10.23 sent 17 packets to 10.10.10.22.