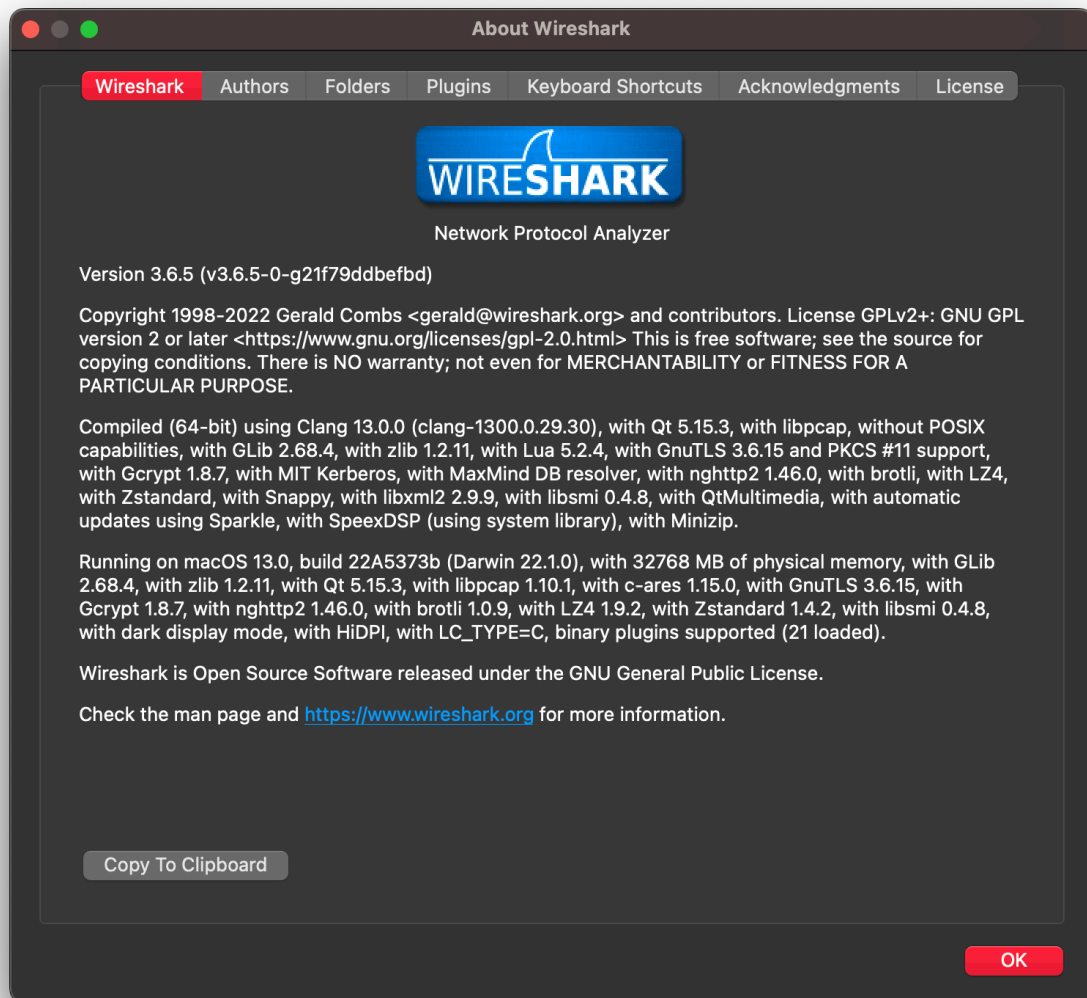
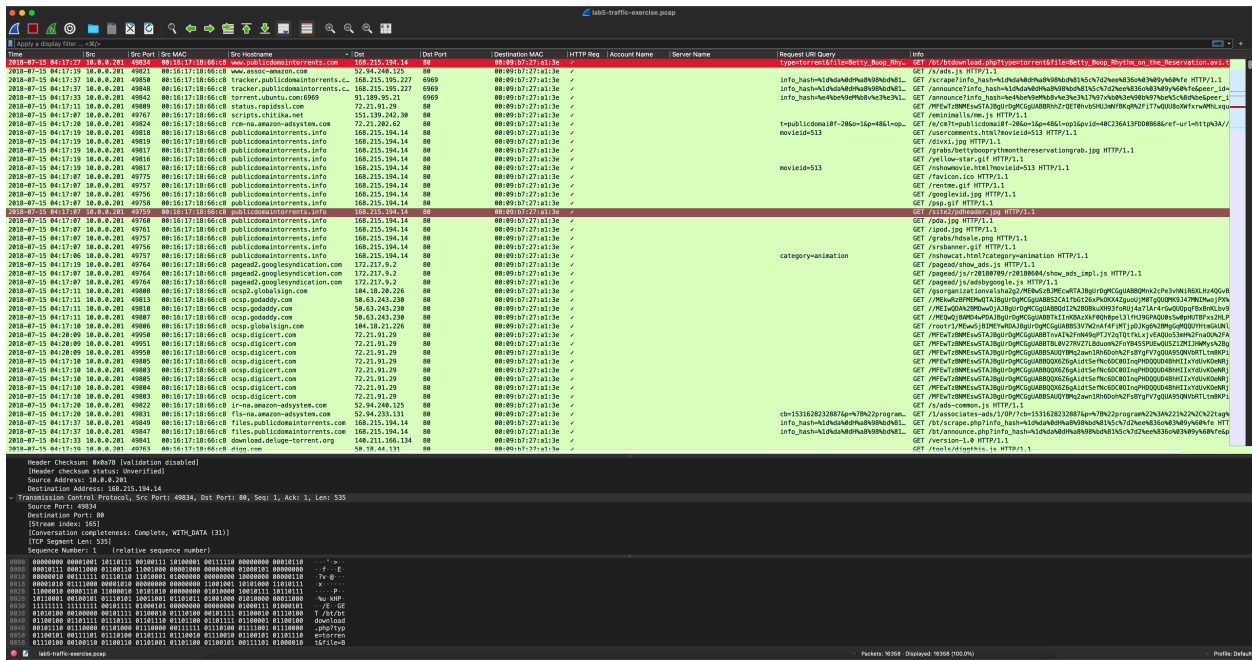


Lab 5
Jonathan Metzger
11/13/22

Step 1



Step 2



Step 3

Filter	Value
MAC address	ip.src == 10.0.0.201 && eth.src 00:16:17:18:66:c8
Hostname/Account	ip.src == 10.0.0.201 && kerberos.CNameString elmer.blanco / BLANCO-DESKTOP
Torrent Hostname	http.host contains torrent "torrent.ubuntu.com:6969"
Torrent File	http.request.uri.query contains file type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent

- What is the MAC address of the computer at 10.0.0.201?

To find the MAC address of 10.0.0.201, I filter “ip.src == 10.0.0.201 && etc.src” and select any row. I look at the “eth.src” to find that the MAC source address Msi_18:66:c8 is 00:16:17:18:66:c8

Time	Src	Src Port	Src MAC
2018-07-15 04:15:42	10.0.0.201		00:16:17:18:66:c8

- What is the host name of the computer at 10.0.0.201?

By looking at the MAC address, I filtered “ip.src == 10.0.0.201 && kerberos.CNameString”. Under DHCP/HostName I found Host Name to be “BLANCO-DESKTOP”. OR same as part 3

3. What is the Windows user account name for the computer at 10.0.0.201?

By looking at the MAC address, I filtered "ip.src == 10.0.0.201 && kerberos.CNameString". Under "Kerberos/as-req/req-body/cname/cname-string" I found Windows User Account name to be "elmer.blanco".

Time	Src	Src Port	Src MAC	Account Name
2018-07-15 04:15:53	10.0.0.201	49741	00:16:17:18:66:c8	BLANCO-DESKTOP\$
2018-07-15 04:15:53	10.0.0.201	49742	00:16:17:18:66:c8	BLANCO-DESKTOP\$
2018-07-15 04:15:43	10.0.0.201	49675	00:16:17:18:66:c8	blanco-desktop\$
2018-07-15 04:15:43	10.0.0.201	49677	00:16:17:18:66:c8	blanco-desktop\$
2018-07-15 04:15:43	10.0.0.201	49678	00:16:17:18:66:c8	blanco-desktop\$
2018-07-15 04:15:43	10.0.0.201	49679	00:16:17:18:66:c8	blanco-desktop\$
2018-07-15 04:15:43	10.0.0.201	49682	00:16:17:18:66:c8	blanco-desktop\$
2018-07-15 04:15:43	10.0.0.201	49683	00:16:17:18:66:c8	blanco-desktop\$
2018-07-15 04:15:43	10.0.0.201	49690	00:16:17:18:66:c8	blanco-desktop\$
2018-07-15 04:15:43	10.0.0.201	49691	00:16:17:18:66:c8	blanco-desktop\$
2018-07-15 04:16:52	10.0.0.201	49744	00:16:17:18:66:c8	elmer.blanco
2018-07-15 04:16:52	10.0.0.201	49745	00:16:17:18:66:c8	elmer.blanco

4. What is the Microsoft Windows version (XP, 7, 8, or 10) of the computer at 10.0.0.201?

By looking at any packet from the IP of 10.0.0.201, and looking at the Hypertext Transfer Protocol/User-Agent, we get “Mozilla/5.0 (Windows NT 10.0; Win64; x64)”.

```

    GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n
  [Expert Info (Chat/Sequence): GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1]
    [GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n]
    [Severity level: Chat]
    [Group: Sequence]
  Request Method: GET
  Request URI: /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
    Request URI Path: /bt/btdownload.php
  Request URI Query: type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
    Request URI Query Parameter: type=torrent
    Request URI Query Parameter: file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
  Request Version: HTTP/1.1
  Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge

```

5. What time in UTC did the torrent activity from 10.0.0.201 start?

http.host contains torrent								
Time	Src	Src Port	Src MAC	Src Hostname	Account Name	Dst	Dst Port	
2018-07-15 04:17:06	10.0.0.201	49757	00:16:17:18:66:c8	publicdomaintorrents.info		168.215.194.14	80	
2018-07-15 04:17:07	10.0.0.201	49756	00:16:17:18:66:c8	publicdomaintorrents.info		168.215.194.14	80	
2018-07-15 04:17:07	10.0.0.201	49757	00:16:17:18:66:c8	publicdomaintorrents.info		168.215.194.14	80	
2018-07-15 04:17:07	10.0.0.201	49761	00:16:17:18:66:c8	publicdomaintorrents.info		168.215.194.14	80	
2018-07-15 04:17:07	10.0.0.201	49760	00:16:17:18:66:c8	publicdomaintorrents.info		168.215.194.14	80	
2018-07-15 04:17:07	10.0.0.201	49759	00:16:17:18:66:c8	publicdomaintorrents.info		168.215.194.14	80	
2018-07-15 04:17:07	10.0.0.201	49758	00:16:17:18:66:c8	publicdomaintorrents.info		168.215.194.14	80	
2018-07-15 04:17:07	10.0.0.201	49756	00:16:17:18:66:c8	publicdomaintorrents.info		168.215.194.14	80	
2018-07-15 04:17:07	10.0.0.201	49757	00:16:17:18:66:c8	publicdomaintorrents.info		168.215.194.14	80	
2018-07-15 04:17:07	10.0.0.201	49775	00:16:17:18:66:c8	publicdomaintorrents.info		168.215.194.14	80	
2018-07-15 04:17:19	10.0.0.201	49817	00:16:17:18:66:c8	publicdomaintorrents.info		168.215.194.14	80	
2018-07-15 04:17:19	10.0.0.201	49816	00:16:17:18:66:c8	publicdomaintorrents.info		168.215.194.14	80	
2018-07-15 04:17:19	10.0.0.201	49817	00:16:17:18:66:c8	publicdomaintorrents.info		168.215.194.14	80	
2018-07-15 04:17:19	10.0.0.201	49819	00:16:17:18:66:c8	publicdomaintorrents.info		168.215.194.14	80	
2018-07-15 04:17:19	10.0.0.201	49818	00:16:17:18:66:c8	publicdomaintorrents.info		168.215.194.14	80	
2018-07-15 04:17:27	10.0.0.201	49834	00:16:17:18:66:c8	www.publicdomaintorrents.com		168.215.194.14	80	
2018-07-15 04:17:33	10.0.0.201	49841	00:16:17:18:66:c8	download.deluge-torrent.org		140.211.166.134	80	
2018-07-15 04:17:33	10.0.0.201	49842	00:16:17:18:66:c8	torrent.ubuntu.com:6969		91.189.95.21	6969	
2018-07-15 04:17:37	10.0.0.201	49847	00:16:17:18:66:c8	files.publicdomaintorrents.com		168.215.194.14	80	
2018-07-15 04:17:37	10.0.0.201	49848	00:16:17:18:66:c8	tracker.publicdomaintorrents.c...		168.215.195.227	6969	
2018-07-15 04:17:37	10.0.0.201	49849	00:16:17:18:66:c8	files.publicdomaintorrents.com		168.215.194.14	80	
2018-07-15 04:17:37	10.0.0.201	49850	00:16:17:18:66:c8	tracker.publicdomaintorrents.c...		168.215.195.227	6969	

bittorrent								
Time	Src	Src Port	Src MAC	Info				
2018-07-15 04:18:08	10.0.0.201	49892	00:16:17:18:66:c8	Handshake				
2018-07-15 04:18:09	128.71.11...	6885	00:09:b7:27:a1:3e	Handshake Bitfield, Len:0x1cb Extended				
2018-07-15 04:18:09	10.0.0.201	49892	00:16:17:18:66:c8	Extended Have All Allowed Fast, Piece (Idx:0x1be) Allowed Fast, Piece (Idx:0x1be)				
2018-07-15 04:18:30	10.0.0.201	49907	00:16:17:18:66:c8	Handshake				
2018-07-15 04:18:30	2.7.43.235	6881	00:09:b7:27:a1:3e	Handshake				
2018-07-15 04:18:30	10.0.0.201	49907	00:16:17:18:66:c8	Extended Have All Allowed Fast, Piece (Idx:0xdf3) Allowed Fast, Piece (Idx:0xdf3)				
2018-07-15 04:18:30	2.7.43.235	6881	00:09:b7:27:a1:3e	Have All Port Extended				
2018-07-15 04:18:32	10.0.0.201	49909	00:16:17:18:66:c8	Handshake				
2018-07-15 04:18:33	121.44.39...	6881	00:09:b7:27:a1:3e	Handshake				
2018-07-15 04:18:33	10.0.0.201	49909	00:16:17:18:66:c8	Extended Have All Allowed Fast, Piece (Idx:0xb4a) Allowed Fast, Piece (Idx:0xb4a)				
2018-07-15 04:19:33	10.0.0.201	49925	00:16:17:18:66:c8	Handshake				
2018-07-15 04:19:33	121.44.39...	6881	00:09:b7:27:a1:3e	Handshake Extended Have All Port				
2018-07-15 04:19:33	10.0.0.201	49925	00:16:17:18:66:c8	Extended Have All Allowed Fast, Piece (Idx:0xb4a) Allowed Fast, Piece (Idx:0xb4a)				

By filtering “http.host contains torrent” for http connections, we can see all packets that relate to torrent activity. We can also filter by using “bittorrent” for TCP connections. The first timestamp for torrent activity is at “2018-07-15 04:17:06” and last timestamp for torrent activity is at “2018-07-15 04:19:33”.

6. What torrent file did the user at 10.0.0.201 download?

By filtering the following: “http.request.uri.query contains file” I was able to find the packets that contain files. This packet was a GET request from /bt/download.php... The only result had the following file: “Betty_Boop_Rhythm_on_the_reservation.avi.torrent”

Hypertext Transfer Protocol	
GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n	
[Expert Info (Chat/Sequence): GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1]	
[GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n]	
[Severity level: Chat]	
[Group: Sequence]	
Request Method: GET	
Request URI: /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent	
Request URI Path: /bt/btdownload.php	
Request URI Query: type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent	
Request URI Query Parameter: type=torrent	
Request URI Query Parameter: file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent	

7. What is the name of the torrent client used on 10.0.0.201?

I searched for different torrent clients at <https://www.vpnmentor.com/blog/best-torrent-clients/> to see what was used in the packets. By filtering “http.host contains torrent” I found under “download.deluge-torrent.org” that the torrent client “Deluge” is being used on IP 10.0.0.201.

8. What file is being seeded (shared) by the torrent client on 10.0.0.201?

By filtering “http.request && http.host” and looking for “torrent.ubuntu.com:6969” I found in Hypertext Transfer Protocol > [truncated] GET /announce?

info_hash=%e4%be%9eM%b8v%e3%e3%17%97x%b0%3e%90b%97%be%5c%8d%be&peer_id=-DE13F0-

VnpZRF8ZP9iv&port=63448&uploaded=0&downloaded=0&left=1921843200&corrupt=0&key=764CA003&event=started&numwant=200&compact=1&no_peer_id. Putting the info_hash into “asciitohex.com” I got the Hexadecimal value of : 65 34 62 65 39 65 4d 62 38 76 65 33 65 33 31 37 39 37 78 62 30 33 65 39 30 62 39 37 62 65 35 63 38 64 62 65

The info_hash can also be found with the “bittorrent” filter

```
▼ BitTorrent
  Protocol Name Length: 19
  Protocol Name: BitTorrent protocol
  Reserved Extension Bytes: 0000000000100005
  SHA1 Hash of info dictionary: e4be9e4db876e3e3179778b03e906297be5c8dbe
  Peer ID: 2d4445313346302d566e705a5246385a50396976
  [Community ID: 1:fcagiTxRiJRvSayyHF/EdVsbFAA=]
```

ASCII to Hex

...and other free text conversion tools

Text (ASCII / ANSI) e4be9e4db876e3e3179778b03e906297be5c8dbe Convert Highlight Text	Binary 01100101 00110100 01100010 01100101 00111001 01100101 01001101 01100010 00111000 01110110 01100101 00110011 01100101 00110011 00110001 00110111 00111001 00110111 01111000 01100010 00110000 00110011 01100101 00111001 00110000 01100010 00111001 00110111 01100010 01100101 00110101 01100011 00111000 01100100 01100010 01100101 Convert Highlight Text	Hexadecimal 65 34 62 65 39 65 4d 62 38 76 65 33 65 33 31 37 39 37 78 62 30 33 65 39 30 62 39 37 62 65 35 63 38 64 62 65 Convert Highlight Text	BASE64 ZTRiZTlITWl4dmUzZTMxNzkeGiwM2U5MGISN2JlNW M4ZGJl Convert Highlight Text
Decimal 101 52 98 101 57 101 77 98 56 118 101 51 101 51 49 55 57 55 120 98 48 51 101 57 48 98 57 55 98 101 53 99 56 100 98 101 Convert Highlight Text	ROT13 r4or9rZo8lr3r3179778b03e906297be5c8dbe Convert Highlight Text	URL Encoded e4be9e4db876e3e3179778b03e906297be5c8dbe Convert Highlight Text	HTML Entities e4be9e4db876e3e3179778b03e906297be5c8dbe Convert Highlight Text