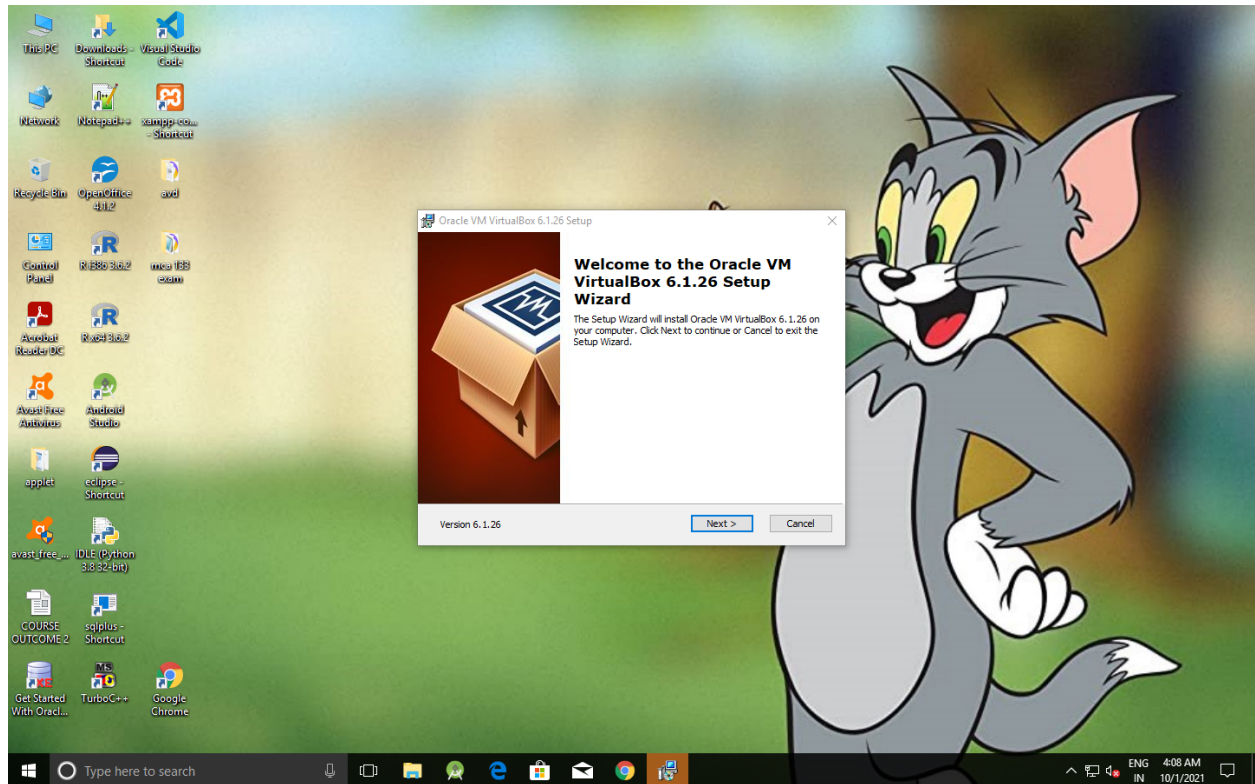
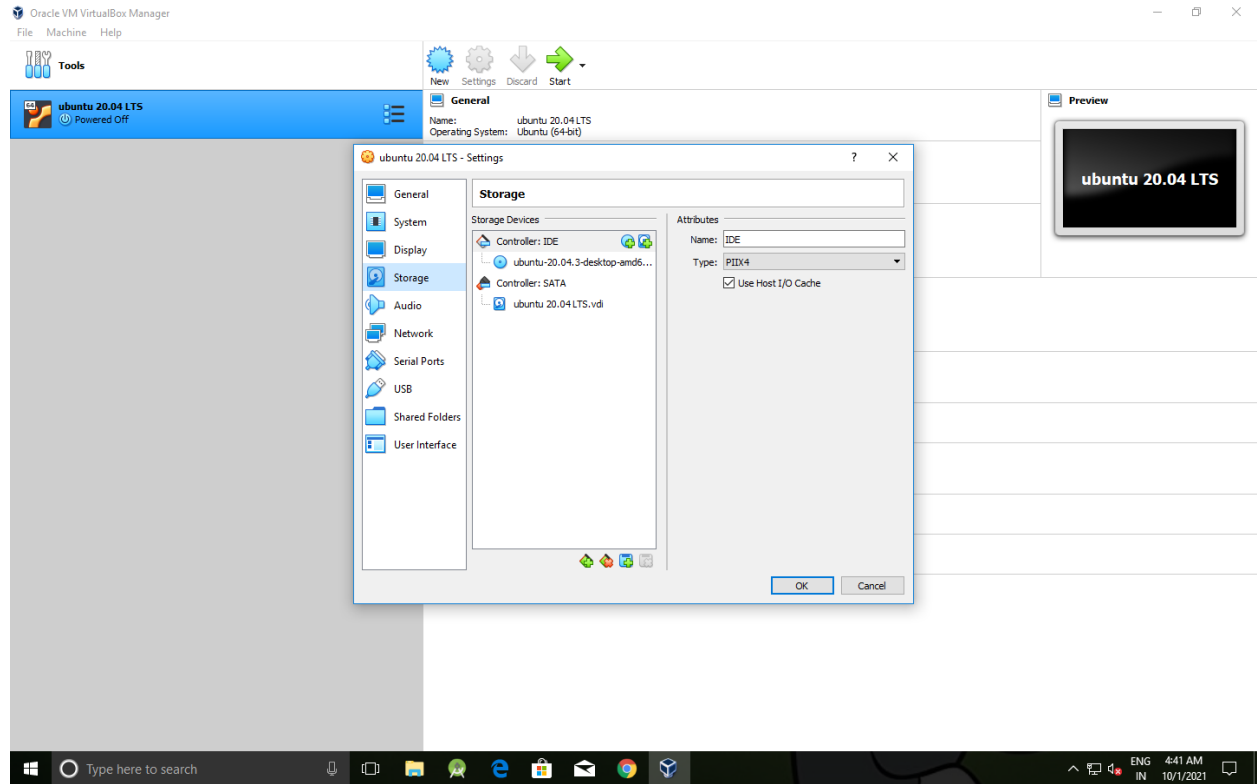


NETWORKING AND SYSTEM ADMINISTRATION SYSTEM
BLESSY P ROY
ROLL NO:214
TKM20MCA-2014

1.





5.

Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
11038	60.980253	172.20.34.54	199.250.200.43	HTTP	637	GET / HTTP/1.1
11118	61.293962	172.20.34.54	199.250.200.43	HTTP	458	GET / HTTP/1.1
11264	61.658841	199.250.200.43	172.20.34.54	HTTP	1310	HTTP/1.1 200 OK (text/html)
11268	61.682041	172.20.34.54	199.250.200.43	HTTP	458	GET /js/ajax-mall.js HTTP/1.1
11336	61.930583	199.250.200.43	172.20.34.54	HTTP	490	HTTP/1.1 404 Not Found (text/html)
11400	62.049707	199.250.200.43	172.20.34.54	HTTP	1310	HTTP/1.1 200 OK (text/html)
11414	62.148240	172.20.34.54	199.250.200.43	HTTP	458	GET /js/ajax-mall.js HTTP/1.1
11558	62.398775	199.250.200.43	172.20.34.54	HTTP	490	HTTP/1.1 404 Not Found (text/html)
11582	62.469167	172.20.34.54	199.250.200.43	HTTP	529	GET /css/color/color-1.css HTTP/1.1
11583	62.472865	172.20.34.54	199.250.200.43	HTTP	554	GET /images/icons/slick-loader.gif HTTP/1.1
11631	62.720135	199.250.200.43	172.20.34.54	HTTP	259	HTTP/1.1 304 Not Modified
11632	62.720573	199.250.200.43	172.20.34.54	HTTP	490	HTTP/1.1 404 Not Found (text/html)
11806	63.032133	172.20.34.54	23.60.169.32	HTTP	334	GET /msdownload/update/v3/static/trusted/en/autorootst1.cab76d833ee7b8546edb HTTP/1.1

> Frame 11808: 637 bytes on wire (5096 bits), 637 bytes captured (5096 bits) on interface \Device\NPF_{FDACC928-7C36-47BF-AB18-980FE4DA576D}, id 0

> Ethernet II, Src: HewlettP_2e:68:20 (f4:39:09:2e:68:20), Dst: Sophos_6b:b3:da (00:1a:8c:6b:b3:da)

> Internet Protocol Version 4, Src: 172.20.34.54, Dst: 199.250.200.43

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 623

Identification: 0x5f05 (24501)

> Flags: 0x40, Don't fragment

Fragment Offset: 0

Time to Live: 128

Protocol: TCP (6)

Header Checksum: 0x3a63 [validation disabled]

[Header checksum status: Unverified]

0000 00 1a 8c 6b b3 da f4 39 09 2e 68 20 00 00 45 00 ...k...h...E

0010 02 6f 9f b5 40 00 00 06 3a 63 ac 14 22 36 c7 fa ...B...ic...5...

0020 c8 2b f2 6f 00 50 a7 b9 62 5a f7 f0 7a 71 50 18 ...oP...bZ...zqP...

0030 01 04 c2 34 00 00 47 45 54 20 2f 20 48 54 54 50 ...4...GE T / HTTP

0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 74 6b 6d 63 /1.1..Ho st: tkmc

0050 65 2e 61 63 2e 69 6e 0d 0a 43 6f 6e 6e 65 63 74 e.ac.in...Connect

0060 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d ion: Kee p-alive

0070 0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 ..Cache-C ontrol:

0080 6d 61 78 2d 61 67 65 3d 30 0d 0a 55 70 67 72 61 max-age= 0...Upgra

0090 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 71 75 de-Insec ure-Requ

00a0 65 73 74 73 3a 20 31 0d 0a 55 73 65 72 2d 41 67 ests: 1 ..User-Ag

00b0 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 ent: Moz illa/5.0

00c0 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e (Window s NT 10..

00d0 30 3b 20 57 69 6e 36 34 3b 20 78 36 34 29 20 41 0; Win64 ; x64) A

00e0 70 70 6c 65 57 65 62 4b 69 74 2f 35 33 37 2e 33 ppleWebK it/537.3

00f0 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 6b 65 20 47 6 (KHTML , like G

Internet Protocol Version 4 (p), 20 bytes

Packets: 194483 · Displayed: 34 (0.0%)

Profile: Default

ENG 5:56 AM 10/1/2021

Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
11583	62.472865	172.20.34.54	199.250.200.43	HTTP	554	GET /images/icons/slick-loader.gif HTTP/1.1
11631	62.720135	199.250.200.43	172.20.34.54	HTTP	259	HTTP/1.1 304 Not Modified
11632	62.720573	199.250.200.43	172.20.34.54	HTTP	490	HTTP/1.1 404 Not Found (text/html)
11806	63.032133	172.20.34.54	23.60.169.32	HTTP	334	GET /msdownload/update/v3/static/trusted/en/autorootst1.cab76d833ee7b8546edb HTTP/1.1
11808	63.032722	23.60.169.32	172.20.34.54	HTTP	320	HTTP/1.1 304 Not Modified
12066	63.967907	172.20.34.54	199.250.200.43	HTTP	565	GET /images/favicon.png HTTP/1.1
12269	64.464747	199.250.200.43	172.20.34.54	HTTP	186	HTTP/1.1 200 OK (PNG)
24077	113.297670	172.20.34.54	103.158.42.57	HTTP	495	GET /academics HTTP/1.1
24095	113.366492	103.158.42.57	172.20.34.54	HTTP	250	HTTP/1.1 302 Object moved (text/html)
24171	113.709949	172.20.34.54	91.199.212.52	HTTP	220	GET /SectigORSASOrganizationValidationSecureServerCA.crt HTTP/1.1
24223	113.922774	91.199.212.52	172.20.34.54	HTTP	735	HTTP/1.1 200 OK (application/pkix-cert)
52825	212.462681	172.20.34.54	77.234.45.70	HTTP	328	GET /R/A2QKIGZ1ZTZh2jYvNzB1ZjRlNmVlHTBkMwVhMThmOTJkZkA0EgQA3hGKwCIgh-KggIB80P4d03At1Rk4SoAUjg6nn1aQahn637v7Au6vkNRDv...
55110	225.640191	172.20.34.54	34.122.121.32	HTTP	141	GET / HTTP/1.1

> Frame 12269: 186 bytes on wire (1488 bits), 186 bytes captured (1488 bits) on interface \Device\NPF_{FDACC928-7C36-47BF-AB18-980FE4DA576D}, id 0

> Ethernet II, Src: Sophos_6b:b3:da (00:1a:8c:6b:b3:da), Dst: HewlettP_2e:68:20 (f4:39:09:2e:68:20)

> Internet Protocol Version 4, Src: 199.250.200.43, Dst: 172.20.34.54

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 172

Identification: 0x4b6 (17590)

> Flags: 0x40, Don't fragment

Fragment Offset: 0

Time to Live: 51

Protocol: TCP (6)

Header Checksum: 0xa425 [validation disabled]

0000 f4 39 09 2e 68 20 00 1a 8c 6b b3 da 00 00 45 00 ...h...k...E

0010 00 ac 44 b6 40 00 33 06 a0 25 c7 fa c8 2b ac 14 ...D...B...3...K...+...

0020 22 38 00 50 f2 6f f7 f1 f8 d1 a7 b9 6a 28 50 18 ...gP...o...j(P...

0030 01 09 4a 79 00 00 08 6e 37 1b e5 9a f0 14 d7 25 ...Jy...n 7...%...

0040 94 6a 23 21 ec 6a f2 24 09 cf a7 49 91 e8 74 48 ...j...l...j...I...th

0050 ca 24 e7 25 3b ba 98 2b 53 ea 2b ff 03 c6 e1 8b ...\$%3...+ S+...+...

0060 5f 09 32 ff 06 ba ff 0f 32 22 f1 3c e1 4c 00 82 ...2...2...2...<L...<

0070 c9 85 5c bb 78 f9 86 9e 00 22 54 c0 1d a4 3d d9 ...X...x...T...=...

0080 f6 58 5b 4e 2e cd 9c 2e b9 9e 87 08 bf 93 3e 4d ...X[N...,...>M...

0090 92 38 c5 73 67 88 f8 1f bd 3d 78 92 08 cb d8 3a ...8...g...x...+...

00a0 b6 0d 46 12 f4 7f 68 58 04 28 f9 cc d9 6b 00 00 ...F...hX...(-...k...<

00b0 00 09 49 45 4e 44 ae 42 60 82 ...IEND: 0 ...

Frame (186 bytes) Reassembled TCP (25332 bytes)

Internet Protocol Version 4 (p), 20 bytes

Packets: 200249 · Displayed: 34 (0.0%)

Profile: Default

ENG 5:57 AM 10/1/2021

Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
55110	225.640191	172.20.34.54	34.122.121.32	HTTP	141	GET / HTTP/1.1
59320	245.630499	172.20.34.54	35.224.170.84	HTTP	141	GET / HTTP/1.1
59381	245.873890	35.224.170.84	172.20.34.54	HTTP	202	HTTP/1.1 204 No Content
84955	376.099733	172.20.34.54	23.60.169.24	HTTP	136	GET /ncc.txt HTTP/1.1
84958	376.112237	23.60.169.24	172.20.34.54	HTTP	205	HTTP/1.1 200 OK (text/html)
1182...	565.612118	172.20.34.54	35.232.111.17	HTTP	141	GET / HTTP/1.1
1182...	565.857733	35.232.111.17	172.20.34.54	HTTP	202	HTTP/1.1 204 No Content
1253...	607.861124	172.20.34.54	77.234.45.88	HTTP	328	GET /R/A2QKIGZ1Z7hZjY4NzB1ZjRlNmVlMTBkMwVhMThmOTJkNzA0EgQAJAkHGWCIgh-KggIB8DP4d0JAT1Rk4SoAUigGnn1aQaIn637vt9Au6vkNRDvz...
1706...	865.703737	172.20.34.54	35.224.170.84	HTTP	141	GET / HTTP/1.1
1706...	865.947124	35.224.170.84	172.20.34.54	HTTP	202	HTTP/1.1 204 No Content
1905...	976.198705	172.20.34.54	23.60.169.35	HTTP	136	GET /ncc.txt HTTP/1.1
1905...	976.213821	23.60.169.35	172.20.34.54	HTTP	205	HTTP/1.1 200 OK (text/html)
1914...	981.241758	172.20.34.54	77.234.45.81	HTTP	328	GET /R/A2QKIGZ1Z7hZjY4NzB1ZjRlNmVlMTBkMwVhMThmOTJkNzA0EgQAJAkHGWCIgh-KggIB8DP4d0JAT1Rk4SoAUigGnn1aQaIn637vt9Au6vkNRDvz...

Frame 84958: 205 bytes on wire (1640 bits), 205 bytes captured (1640 bits) on interface \Device\NPF_{FDACC928-7C36-47BF-AB18-90DFE4DA576D}, id 0

> Interface id: 0 (\Device\NPF_{FDACC928-7C36-47BF-AB18-90DFE4DA576D})

Encapsulation type: Ethernet (1)

Arrival Time: Oct 1, 2021 05:46:26.714145000 Pacific Daylight Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1633092386.714145000 seconds

[Time delta from previous captured frame: 0.011319000 seconds]

[Time delta from previous displayed frame: 0.012504000 seconds]

[Time since reference or first frame: 376.112237000 seconds]

Frame Number: 84958

Frame Length: 205 bytes (1640 bits)

Capture Length: 205 bytes (1640 bits)

[Frame is marked: False]

[Frame is ignored: False]

0000 f4 39 09 2e 68 20 00 1a 8c 6b b3 da 08 00 45 00 :9..h...k...E-

0010 00 bf 90 7d 00 00 3d 06 5e 1d 17 3c a9 18 ac 14 :...}...-...k...-...

0020 22 36 00 50 f2 12 18 c9 e6 eb 71 af a0 0c 50 18 :g P...-...q...P-

0030 00 e5 ce 38 00 00 48 54 54 50 2f 31 2e 31 20 32 :--8--HT TP/1.1 2

0040 30 30 20 4f 4b 0d 0a 43 6f 6e 74 65 6e 74 2d 54 :00 OK-C content-T

0050 79 70 65 3a 20 74 65 78 74 2f 68 74 6d 6c 0d 0a :ype: tex t/html-

0060 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 :Content- Length:

0070 32 36 0d 0a 44 61 74 65 3a 20 46 72 69 2c 20 30 :26--Date : Fri, 0

0080 31 20 4f 63 74 20 32 30 32 31 20 30 35 3a 34 36 :1 Oct 20 21 05:46

0090 3a 32 35 20 47 4d 54 0d 0a 43 6f 6e 6e 65 63 74 :;25 GMT--Connect

00a0 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d :ion: Kee p-alive-

00b0 0a 0d 0a 4e 65 74 77 6f 72 6b 28 43 6f 6e 6e 65 :--Netwo rk Conne

00c0 63 74 69 76 69 74 79 20 43 68 65 63 6b :ctivity Check

Internet Protocol Version 4 (IP), 20 bytes

Packets: 211763 · Displayed: 34 (0.0%)

Profile: Default

ENG 5:58 AM 10/1/2021

Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
24095	113.366492	103.158.42.57	172.20.34.54	HTTP	250	HTTP/1.1 302 Object moved (text/html)
24171	113.709949	172.20.34.54	91.199.212.52	HTTP	220	GET /SectionRSAOrganizationValidationSecureServerCA.crt HTTP/1.1
24223	113.922774	91.199.212.52	172.20.34.54	HTTP	735	HTTP/1.1 200 OK (application/pkix-cert)
52825	212.462681	172.20.34.54	77.234.45.70	HTTP	328	GET /R/A2QKIGZ1Z7hZjY4NzB1ZjRlNmVlMTBkMwVhMThmOTJkNzA0EgQAJAkHGWCIgh-KggIB8DP4d0JAT1Rk4SoAUigGnn1aQaIn637vt9Au6vkNRDvz...
55110	225.640191	172.20.34.54	34.122.121.32	HTTP	141	GET / HTTP/1.1
59320	245.630499	172.20.34.54	35.224.170.84	HTTP	141	GET / HTTP/1.1
59381	245.873890	35.224.170.84	172.20.34.54	HTTP	202	HTTP/1.1 204 No Content
84955	376.099733	172.20.34.54	23.60.169.24	HTTP	136	GET /ncc.txt HTTP/1.1
84958	376.112237	23.60.169.24	172.20.34.54	HTTP	205	HTTP/1.1 200 OK (text/html)
1182...	565.612118	172.20.34.54	35.232.111.17	HTTP	141	GET / HTTP/1.1
1182...	565.857733	35.232.111.17	172.20.34.54	HTTP	202	HTTP/1.1 204 No Content
1253...	607.861124	172.20.34.54	77.234.45.88	HTTP	328	GET /R/A2QKIGZ1Z7hZjY4NzB1ZjRlNmVlMTBkMwVhMThmOTJkNzA0EgQAJAkHGWCIgh-KggIB8DP4d0JAT1Rk4SoAUigGnn1aQaIn637vt9Au6vkNRDvz...
1706...	865.703737	172.20.34.54	35.224.170.84	HTTP	141	GET / HTTP/1.1

Frame 170605: 141 bytes on wire (1128 bits), 141 bytes captured (1128 bits) on interface \Device\NPF_{FDACC928-7C36-47BF-AB18-90DFE4DA576D}, id 0

> Ethernet II, Src: HewlettP_2e:68:20 (f4:39:09:2e:68:20), Dst: Sophos_6b:b3:da (00:1a:8c:6b:b3:da)

> Internet Protocol Version 4, Src: 172.20.34.54, Dst: 35.224.170.84

> Transmission Control Protocol, Src Port: 52007, Dst Port: 80, Seq: 1, Ack: 1, Len: 87

> Hypertext Transfer Protocol

0000 00 1a 8c 6b b3 da f4 39 09 2e 68 20 08 00 45 00 :...k...9...h...E-

0010 00 7f 4e 9a 40 00 00 06 0f 60 ac 14 22 36 23 e6 :...N@... .."58-

0020 aa 54 cb 27 00 50 6b f0 d8 1c 5d 98 ce 9f 50 18 :-T..Pk-...-P-

0030 ff f0 16 01 00 00 47 45 54 20 2f 20 48 54 54 50 :.....GE T / HTTP

0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 63 6f 6e 6e :/1.1--Ho st: conn

0050 65 63 74 69 76 69 74 79 2d 63 68 65 63 60 2e 75 :ectivity-check.u

0060 62 75 6e 74 75 2e 63 6f 6d 0d 0a 41 63 63 65 70 :untu.co m--Accop

0070 74 3a 20 2a 2f 2a 9d 0a 43 6f 6e 6e 65 63 74 69 :ti: /*-- Connecti

0080 6f 6e 3a 20 63 6c 6f 73 65 0d 0a 0d 0a :on: clos e--...

Frame (Frame), 141 bytes

Packets: 218147 · Displayed: 34 (0.0%)

Profile: Default

ENG 5:59 AM 10/1/2021