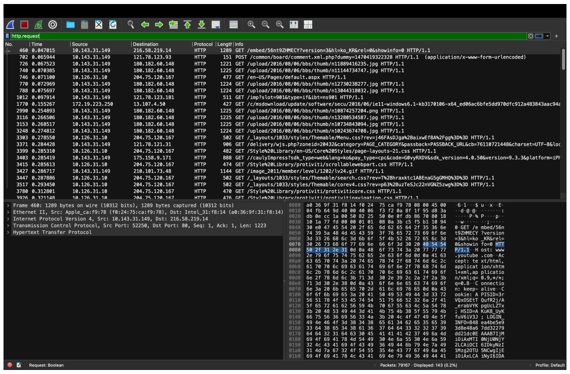
IOT_Midterm_Exam
Lakshminath Reddy Alamuru
SUID: 367982169

Task given in the Blackboard by using the Wireshark tool

1. Filtered the http request



http.request

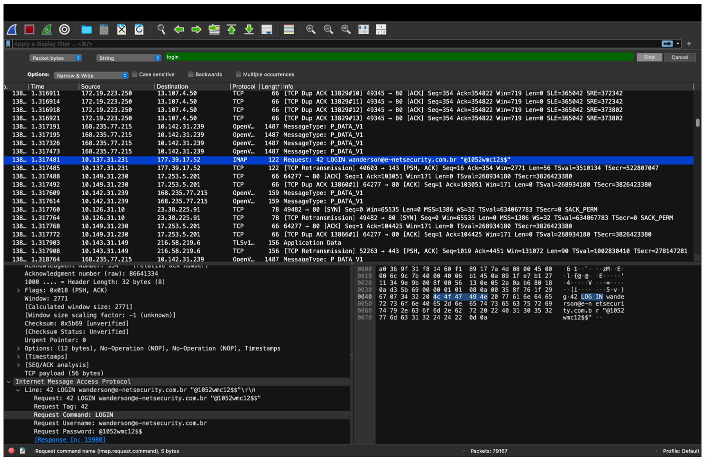
```
No.  Time      Source          Destination     Protocol Length Info
 460 0.047015  10.143.31.149   216.58.219.14   HTTP  1289 GET /embed/56nt9ZHMECY?version=3&hl=ko_KR&rel=0&showinfo=0 HTTP/1.1
 702 0.065944  10.143.31.149   121.78.123.93   HTTP   151 POST /common/board/comment.xml.php?dummy=1470419322328 HTTP/1.1  (application/x-www-form-urlencoded)
 726 0.067523  10.143.31.149   180.182.60.148  HTTP  1221 GET /upload/2016/08/06/bbs/thumb/n11889416235.jpg HTTP/1.1
 740 0.070385  10.143.31.149   180.182.60.148  HTTP  1225 GET /upload/2016/08/06/bbs/thumb/n11144734747.jpg HTTP/1.1
 746 0.071100  10.126.31.10    204.75.120.167  HTTP   477 GET /en-US/Pages/default.aspx HTTP/1.1
 770 0.072969  10.143.31.149   180.182.60.148  HTTP  1224 GET /upload/2016/08/06/bbs/thumb/n12730238277.jpg HTTP/1.1
 788 0.075697  10.143.31.149   180.182.60.148  HTTP  1224 GET /upload/2016/08/06/bbs/thumb/n13044318032.jpg HTTP/1.1
1012 0.097914  10.143.31.149   121.78.123.181  HTTP   511 GET /imp?slot=901&type=if&ibt=ns901 HTTP/1.1
1770 0.155267  172.19.223.250  13.107.4.50     HTTP   427 GET /c/msdownload/update/software/secu/2016/06/ie11-windows6.1-kb3170106-x64_ed06ac6bfe5dd970dfc912a483843aac94a
2990 0.254893  10.143.31.149   180.182.60.148  HTTP  1225 GET /upload/2016/08/06/bbs/thumb/n10874257204.png HTTP/1.1
3116 0.266506  10.143.31.149   180.182.60.148  HTTP  1225 GET /upload/2016/08/06/bbs/thumb/n13280534587.jpg HTTP/1.1
3153 0.268517  10.143.31.149   180.182.60.148  HTTP  1225 GET /upload/2016/08/06/bbs/thumb/n10734843094.jpg HTTP/1.1
3248 0.274812  10.143.31.149   180.182.60.148  HTTP  1224 GET /upload/2016/08/06/bbs/thumb/n10243674708.jpg HTTP/1.1
3303 0.278550  10.126.31.10    204.75.120.167  HTTP   502 GET /_layouts/1033/styles/Themable/Menu.css?rev=j46FAsDJga%2BaixwEf8A%2Fgg%3D%3D HTTP/1.1
3371 0.284428  10.143.31.149   121.78.121.31   HTTP   906 GET /delivery/wjs.php?zoneid=20432&category=PAGE_CATEGORY&passback=PASSBACK_URL&cb=76110721448&charset=UTF-8&loc
3399 0.285310  10.126.31.10    204.75.120.167  HTTP   482 GET /Style%20Library/en-US/Core%20Styles/page-layouts-21.css HTTP/1.1
3403 0.285419  10.143.31.149   175.158.9.171   HTTP   888 GET //caulyImpress?sdk_type=web&lang=ko&pay_type=cpc&code=G0vyRXDV&sdk_version=4.0.50&version=9.3.3&platform=iPh
3415 0.285613  10.126.31.10    204.75.120.167  HTTP   474 GET /Style%20Library/protiviti/scrollablewebpart.css HTTP/1.1
3427 0.286717  10.143.31.149   210.101.73.48   HTTP  1144 GET /image_2011/member/level/1202/lv24.gif HTTP/1.1
3447 0.287886  10.126.31.10    204.75.120.167  HTTP   502 GET /_layouts/1033/styles/Themable/search.css?rev=T%2Bhraxktc1A8EnaG5gGMHQ%3D%3D HTTP/1.1
3517 0.293450  10.126.31.10    204.75.120.167  HTTP   502 GET /_layouts/1033/styles/Themable/corev4.css?rev=p63%2BuzTeSJc22nVGNZ5zwg%3D%3D HTTP/1.1
3780 0.312801  10.126.31.10    204.75.120.167  HTTP   470 GET /Style%20Library/protiviti/protiviticore.css HTTP/1.1
3926 0.321148  10.126.31.10    204.75.120.167  HTTP   476 GET /Style%20Library/protiviti/protivitinavigation.css HTTP/1.1
```

```
> Frame 460: 1289 bytes on wire (10312 bits), 1289 bytes captured (10312 bits)
> Ethernet II, Src: Apple_ca:f9:78 (f0:24:75:ca:f9:78), Dst: Intel_31:f8:14 (a0:36:9f:31:f8:14)
> Internet Protocol Version 4, Src: 10.143.31.149, Dst: 216.58.219.14
> Transmission Control Protocol, Src Port: 52250, Dst Port: 80, Seq: 1, Ack: 1, Len: 1223
> Hypertext Transfer Protocol
```

```
0000  a0 36 9f 31 f8 14 f0 24  75 ca f9 78 08 00 45 00   ·6·1···$ u··x··E·
0010  04 fb 64 9d 40 00 40 06  f3 f2 0a 8f 1f 95 d8 3a   ··d·@·@· ·······:
0020  db 0e cc 1a 00 50 82 25  50 0e 0f db 86 70 80 18   ·····P·% P····p··
0030  10 1a 77 fd 00 00 01 01  08 0a 3b c5 f5 b1 10 94   ··w····· ··;·····
0040  30 e0 47 45 54 20 2f 65  6d 62 65 64 2f 35 36 6e   0·GET /e mbed/56n
0050  74 39 5a 48 4d 45 43 59  3f 76 65 72 73 69 6f 6e   t9ZHMECY ?version
0060  3d 33 26 68 6c 3d 6b 6f  5f 4b 52 26 72 65 6c 3d   =3&hl=ko _KR&rel=
0070  30 26 73 68 6f 77 69 6e  66 6f 3d 30 20 48 54 54   0&showin fo=0 HTT
0080  50 2f 31 2e 31 0d 0a 48  6f 73 74 3a 20 77 77 77   P/1.1··H ost: www
0090  2e 79 6f 75 74 75 62 65  2e 63 6f 6d 0d 0a 41 63   .youtube .com··Ac
00a0  63 65 70 74 3a 20 74 65  78 74 2f 68 74 6d 6c 2c   cept: te xt/html,
00b0  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 68 74 6d   applicat ion/xhtm
00c0  6c 2b 78 6d 6c 2c 61 70  70 6c 69 63 61 74 69 6f   l+xml,ap plicatio
00d0  6e 2f 78 6d 6c 3b 71 3d  30 2e 39 2c 2a 2f 2a 3b   n/xml;q= 0.9,*/*;
00e0  71 3d 30 2e 38 0d 0a 43  6f 6e 6e 65 63 74 69 6f   q=0.8··C onnectio
00f0  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 43   n: keep- alive··C
0100  6f 6f 6b 69 65 3a 20 41  50 49 53 49 44 3d 33 72   ookie: A PISID=3r
0110  56 51 78 4f 53 45 74 54  51 75 66 52 32 6a 2f 41   VQxOSEtT QufR2j/A
0120  5f 65 72 61 62 56 59 4b  70 67 55 63 4c 5a 54 78   _erabVYK pgUcLZTx
0130  3b 20 48 53 49 44 3d 41  4b 75 4b 38 5f 55 79 4b   ; HSID=A KuK8_UyK
0140  66 75 56 36 69 56 33 4a  3b 20 4c 4f 47 49 4e 5f   fuV6iV3J ; LOGIN_
0150  49 4e 46 4f 3d 38 34 38  65 61 34 62 65 35 65 39   INFO=848 ea4be5e9
0160  33 64 38 65 34 38 61 36  37 64 64 33 32 32 37 39   3d8e48a6 7dd32279
0170  64 64 32 31 64 63 30 45  41 41 41 42 37 49 6a 4d   dd21dc0E AAAB7IjM
0180  69 4f 69 41 78 4d 54 49  30 4e 6a 55 30 4e 6a 59   iOiAxMTI 0NjU0NjY
0190  32 4c 43 41 69 4f 43 49  36 49 44 6b 79 4e 7a 49   2LCAiOCI 6IDkyNzI
01a0  31 4d 7a 67 32 4f 54 55  35 4e 43 77 67 49 6a 45   1Mzg2OTU 5NCwgIjE
01b0  69 4f 69 41 78 4c 43 41  69 4e 79 49 36 49 44 41   iOiAxLCA iNyI6IDA
```

Request: Boolean · Packets: 79167 · Displayed: 143 (0.2%) · Profile: Default

2. Used IMAP protocol for username:password pair .



Apply a display filter ... <⌘/>

Packet bytes · String · login · Find · Cancel

Options: Narrow & Wide · □ Case sensitive · □ Backwards · □ Multiple occurrences

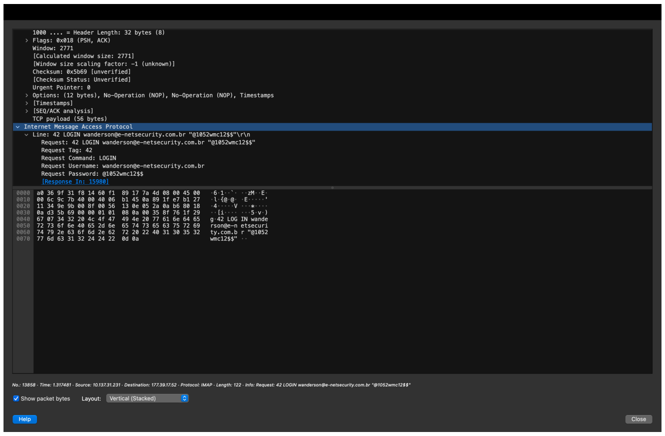
```
No.   Time      Source          Destination     Protocol Length Info
138…  1.316911  172.19.223.250  13.107.4.50     TCP     66  [TCP Dup ACK 13829#10] 49345 → 80 [ACK] Seq=354 Ack=354822 Win=719 Len=0 SLE=365042 SRE=372342
138…  1.316914  172.19.223.250  13.107.4.50     TCP     66  [TCP Dup ACK 13829#11] 49345 → 80 [ACK] Seq=354 Ack=354822 Win=719 Len=0 SLE=365042 SRE=372342
138…  1.316918  172.19.223.250  13.107.4.50     TCP     66  [TCP Dup ACK 13829#12] 49345 → 80 [ACK] Seq=354 Ack=354822 Win=719 Len=0 SLE=365042 SRE=373802
138…  1.316921  172.19.223.250  13.107.4.50     TCP     66  [TCP Dup ACK 13829#13] 49345 → 80 [ACK] Seq=354 Ack=354822 Win=719 Len=0 SLE=365042 SRE=373802
138…  1.317191  168.235.77.215  10.142.31.239   OpenV…  1487 MessageType: P_DATA_V1
138…  1.317195  168.235.77.215  10.142.31.239   OpenV…  1487 MessageType: P_DATA_V1
138…  1.317326  168.235.77.215  10.142.31.239   OpenV…  1487 MessageType: P_DATA_V1
138…  1.317473  168.235.77.215  10.142.31.239   OpenV…  1487 MessageType: P_DATA_V1
138…  1.317481  10.137.31.231   177.39.17.52    IMAP    122 Request: 42 LOGIN wanderson@e-netsecurity.com.br "@1052wmc12$$"
138…  1.317485  10.137.31.231   177.39.17.52    TCP     122 [TCP Retransmission] 40603 → 143 [PSH, ACK] Seq=16 Ack=354 Win=2771 Len=56 TSval=3510134 TSecr=522807047
138…  1.317488  10.149.31.230   17.253.5.201    TCP     66  64277 → 80 [ACK] Seq=1 Ack=103051 Win=171 Len=0 TSval=268934180 TSecr=3826423380
138…  1.317492  10.149.31.230   17.253.5.201    TCP     66  [TCP Dup ACK 13860#1] 64277 → 80 [ACK] Seq=1 Ack=103051 Win=171 Len=0 TSval=268934180 TSecr=3826423380
138…  1.317609  10.142.31.239   168.235.77.215  OpenV…  159 MessageType: P_DATA_V1
138…  1.317614  10.142.31.239   168.235.77.215  OpenV…  159 MessageType: P_DATA_V1
138…  1.317760  10.126.31.10    23.38.225.91    TCP     78  49482 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1386 WS=32 TSval=634067783 TSecr=0 SACK_PERM
138…  1.317764  10.126.31.10    23.38.225.91    TCP     78  [TCP Retransmission] 49482 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1386 WS=32 TSval=634067783 TSecr=0 SACK_PERM
138…  1.317768  10.149.31.230   17.253.5.201    TCP     66  64277 → 80 [ACK] Seq=1 Ack=104425 Win=171 Len=0 TSval=268934180 TSecr=3826423380
138…  1.317772  10.149.31.230   17.253.5.201    TCP     66  [TCP Dup ACK 13866#1] 64277 → 80 [ACK] Seq=1 Ack=104425 Win=171 Len=0 TSval=268934180 TSecr=3826423380
138…  1.317903  10.143.31.149   216.58.219.6    TLSv1…  156 Application Data
138…  1.317908  10.143.31.149   216.58.219.6    TCP     156 [TCP Retransmission] 52263 → 443 [PSH, ACK] Seq=1019 Ack=4451 Win=131072 Len=90 TSval=1002830410 TSecr=278147281
138…  1.318764  168.235.77.215  10.142.31.239   OpenV…  1487 MessageType: P_DATA_V1
```

```
    Acknowledgment number (raw): 86641334
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x018 (PSH, ACK)
    Window: 2771
    [Calculated window size: 2771]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x5b69 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (56 bytes)
v Internet Message Access Protocol
  v Line: 42 LOGIN wanderson@e-netsecurity.com.br "@1052wmc12$$"\r\n
      Request: 42 LOGIN wanderson@e-netsecurity.com.br "@1052wmc12$$"
      Request Tag: 42
      Request Command: LOGIN
      Request Username: wanderson@e-netsecurity.com.br
      Request Password: @1052wmc12$$
      [Response In: 15980]
```

```
0000  a0 36 9f 31 f8 14 60 f1  89 17 7a 4d 08 00 45 00   ·6·1··`· ··zM··E·
0010  00 6c 9c 7b 40 00 40 06  b1 45 0a 89 1f e7 b1 27   ·l·{@·@· ·E·····'
0020  11 34 9e 9b 00 8f 00 56  13 0e 05 2a 0a b6 80 18   ·4·····V ···*····
0030  0a d3 5b 69 00 00 01 01  08 0a 00 35 8f 76 1f 29   ··[i···· ···5·v·)
0040  67 07 34 32 20 4c 4f 47  49 4e 20 77 61 6e 64 65   g·42 LOG IN wande
0050  72 73 6f 6e 40 65 2d 6e  65 74 73 65 63 75 72 69   rson@e-n etsecuri
0060  74 79 2e 63 6f 6d 2e 62  72 20 22 40 31 30 35 32   ty.com.b r "@1052
0070  77 6d 63 31 32 24 24 22  0d 0a                    wmc12$$" ··
```

Request command name (imap.request.command), 5 bytes · Packets: 79167 · Profile: Default

3. Shown in the screenshot, Username : wanderson@e-netsecurituy.com.br, Password: @1052wmc12$$



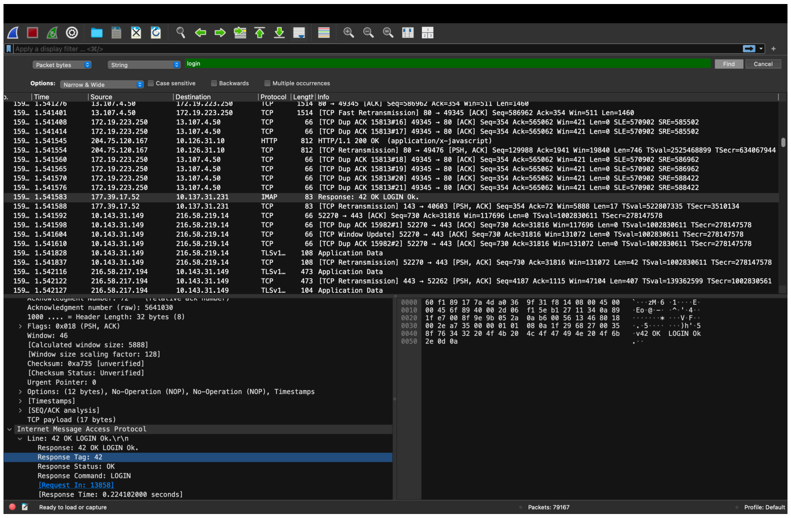
```
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x018 (PSH, ACK)
    Window: 2771
    [Calculated window size: 2771]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x5b69 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (56 bytes)
v Internet Message Access Protocol
  v Line: 42 LOGIN wanderson@e-netsecurity.com.br "@1052wmc12$$"\r\n
      Request: 42 LOGIN wanderson@e-netsecurity.com.br "@1052wmc12$$"
      Request Tag: 42
      Request Command: LOGIN
      Request Username: wanderson@e-netsecurity.com.br
      Request Password: @1052wmc12$$
      [Response In: 15980]
```

```
0000  a0 36 9f 31 f8 14 60 f1  89 17 7a 4d 08 00 45 00   ·6·1··`· ··zM··E·
0010  00 6c 9c 7b 40 00 40 06  b1 45 0a 89 1f e7 b1 27   ·l·{@·@· ·E·····'
0020  11 34 9e 9b 00 8f 00 56  13 0e 05 2a 0a b6 80 18   ·4·····V ···*····
0030  0a d3 5b 69 00 00 01 01  08 0a 00 35 8f 76 1f 29   ··[i···· ···5·v·)
0040  67 07 34 32 20 4c 4f 47  49 4e 20 77 61 6e 64 65   g·42 LOG IN wande
0050  72 73 6f 6e 40 65 2d 6e  65 74 73 65 63 75 72 69   rson@e-n etsecuri
0060  74 79 2e 63 6f 6d 2e 62  72 20 22 40 31 30 35 32   ty.com.b r "@1052
0070  77 6d 63 31 32 24 24 22  0d 0a                    wmc12$$" ··
```

No.: 13858 · Time: 1.317481 · Source: 10.137.31.231 · Destination: 177.39.17.52 · Protocol: IMAP · Length: 122 · Info: Request: 42 LOGIN wanderson@e-netsecurity.com.br "@1052wmc12$$"

☑ Show packet bytes · Layout: Vertical (Stacked)

4. It got respond as ok, login ok 15980 packet



Apply a display filter … <⌘/>

Packet bytes | String | login | Find | Cancel

Options: Narrow & Wide □ Case sensitive □ Backwards □ Multiple occurrences

```
No.   Time      Source          Destination     Protocol Length Info
159…  1.541276  13.107.4.50     172.19.223.250  TCP      1514 80 → 49345 [ACK] Seq=586962 Ack=354 Win=511 Len=1460
159…  1.541401  13.107.4.50     172.19.223.250  TCP      1514 [TCP Fast Retransmission] 80 → 49345 [ACK] Seq=586962 Ack=354 Win=511 Len=1460
159…  1.541408  172.19.223.250  13.107.4.50     TCP        66 [TCP Dup ACK 15813#16] 49345 → 80 [ACK] Seq=354 Ack=565062 Win=421 Len=0 SLE=570902 SRE=585502
159…  1.541414  172.19.223.250  13.107.4.50     TCP        66 [TCP Dup ACK 15813#17] 49345 → 80 [ACK] Seq=354 Ack=565062 Win=421 Len=0 SLE=570902 SRE=585502
159…  1.541545  204.75.120.167  10.126.31.10    HTTP      812 HTTP/1.1 200 OK  (application/x-javascript)
159…  1.541554  204.75.120.167  10.126.31.10    TCP       812 [TCP Retransmission] 80 → 49476 [PSH, ACK] Seq=129988 Ack=1941 Win=19840 Len=746 TSval=2525468899 TSecr=634067944
159…  1.541560  172.19.223.250  13.107.4.50     TCP        66 [TCP Dup ACK 15813#18] 49345 → 80 [ACK] Seq=354 Ack=565062 Win=421 Len=0 SLE=570902 SRE=586962
159…  1.541565  172.19.223.250  13.107.4.50     TCP        66 [TCP Dup ACK 15813#19] 49345 → 80 [ACK] Seq=354 Ack=565062 Win=421 Len=0 SLE=570902 SRE=586962
159…  1.541570  172.19.223.250  13.107.4.50     TCP        66 [TCP Dup ACK 15813#20] 49345 → 80 [ACK] Seq=354 Ack=565062 Win=421 Len=0 SLE=570902 SRE=588422
159…  1.541576  172.19.223.250  13.107.4.50     TCP        66 [TCP Dup ACK 15813#21] 49345 → 80 [ACK] Seq=354 Ack=565062 Win=421 Len=0 SLE=570902 SRE=588422
159…  1.541583  177.39.17.52    10.137.31.231   IMAP       83 Response: 42 OK LOGIN Ok.
159…  1.541588  177.39.17.52    10.137.31.231   TCP        83 [TCP Retransmission] 143 → 40603 [PSH, ACK] Seq=354 Ack=72 Win=5888 Len=17 TSval=522807335 TSecr=3510134
159…  1.541592  10.143.31.149   216.58.219.14   TCP        66 52270 → 443 [ACK] Seq=730 Ack=31816 Win=117696 Len=0 TSval=1002830611 TSecr=278147578
159…  1.541598  10.143.31.149   216.58.219.14   TCP        66 [TCP Dup ACK 15982#1] 52270 → 443 [ACK] Seq=730 Ack=31816 Win=117696 Len=0 TSval=1002830611 TSecr=278147578
159…  1.541604  10.143.31.149   216.58.219.14   TCP        66 [TCP Window Update] 52270 → 443 [ACK] Seq=730 Ack=31816 Win=131072 Len=0 TSval=1002830611 TSecr=278147578
159…  1.541610  10.143.31.149   216.58.219.14   TCP        66 [TCP Dup ACK 15982#2] 52270 → 443 [ACK] Seq=730 Ack=31816 Win=131072 Len=0 TSval=1002830611 TSecr=278147578
159…  1.541828  10.143.31.149   216.58.219.14   TLSv1…    108 Application Data
159…  1.541837  10.143.31.149   216.58.219.14   TCP       108 [TCP Retransmission] 52270 → 443 [PSH, ACK] Seq=730 Ack=31816 Win=131072 Len=42 TSval=1002830611 TSecr=278147578
159…  1.542116  216.58.217.194  10.143.31.149   TLSv1…    473 Application Data
159…  1.542122  216.58.217.194  10.143.31.149   TCP       473 [TCP Retransmission] 443 → 52262 [PSH, ACK] Seq=4187 Ack=1115 Win=47104 Len=407 TSval=139362599 TSecr=1002830561
159…  1.542127  216.58.217.194  10.143.31.149   TLSv1…    104 Application Data
```

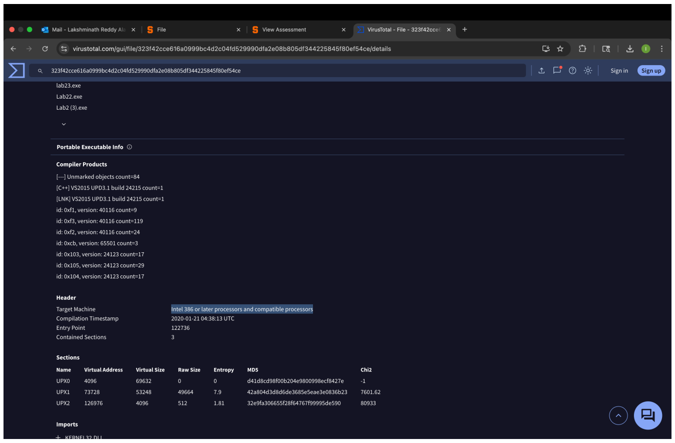
```
    Acknowledgment Number: 72    (relative ack number)
    Acknowledgment number (raw): 5641030
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x018 (PSH, ACK)
    Window: 46
    [Calculated window size: 5888]
    [Window size scaling factor: 128]
    Checksum: 0xa735 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  > [Timestamps]
  > [SEQ/ACK analysis]
    TCP payload (17 bytes)
v Internet Message Access Protocol
  v Line: 42 OK LOGIN Ok.\r\n
      Response: 42 OK LOGIN Ok.
      Response Tag: 42
      Response Status: OK
      Response Command: LOGIN
      [Request In: 13858]
      [Response Time: 0.224102000 seconds]
```

```
0000  60 f1 89 17 7a 4d a0 36  9f 31 f8 14 08 00 45 00   `···zM·6 ·1····E·
0010  00 45 6f 89 40 00 2d 06  f1 5e b1 27 11 34 0a 89   ·Eo·@·-· ·^·'·4··
0020  1f e7 00 8f 9e 9b 05 2a  0a b6 00 56 13 46 80 18   ·······* ···V·F··
0030  00 2e a7 35 00 00 01 01  08 0a 1f 29 68 27 00 35   ·.·5···· ···)h'·5
0040  8f 76 34 32 20 4f 4b 20  4c 4f 47 49 4e 20 4f 6b   ·v42 OK  LOGIN Ok
0050  2e 0d 0a                                           .··
```

Ready to load or capture | Packets: 79167 | Profile: Default

Part - 2

1. I have used virus total tool, it has shown clear data in the website by pasting the given hash value. Targeted machine - Intel 386 or later processors and compatible processors and the entry point - 122736, Imports - KERNEL32.DLL



virustotal.com/gui/file/323f42cce616a0999bc4d2c04fd529990dfa2e08b805df344225845f80ef54ce/details

323f42cce616a0999bc4d2c04fd529990dfa2e08b805df344225845f80ef54ce

lab23.exe
Lab22.exe
Lab2 (3).exe

Portable Executable Info

Compiler Products

[---] Unmarked objects count=84
[C++] VS2015 UPD3.1 build 24215 count=1
[LNK] VS2015 UPD3.1 build 24215 count=1
id: 0xf1, version: 40116 count=9
id: 0xf3, version: 40116 count=119
id: 0xf2, version: 40116 count=24
id: 0xcb, version: 65501 count=3
id: 0x103, version: 24123 count=17
id: 0x105, version: 24123 count=29
id: 0x104, version: 24123 count=17

Header

Target Machine	Intel 386 or later processors and compatible processors
Compilation Timestamp	2020-01-21 04:38:13 UTC
Entry Point	122736
Contained Sections	3

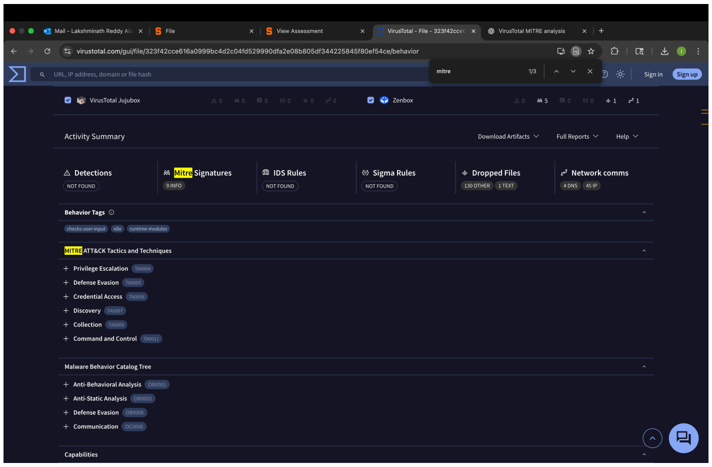
Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
UPX0	4096	69632	0	0	d41d8cd98f00b204e9800998ecf8427e	-1
UPX1	73728	53248	49664	7.9	42a804d3d8d6de3685e5eae3e0836b23	7601.62
UPX2	126976	4096	512	1.81	32e9fa306655f28f64767f99995de590	80933

Imports

+ KERNEL32.DLL

2. It can be seen in the behavior tab and search for mitre. It has shown data


Mail - Lakshminath Reddy Ala
File
View Assessment
VirusTotal - File - 323f42cce6
VirusTotal MITRE analysis
virustotal.com/gui/file/323f42cce616a0999bc4d2c04fd529990dfa2e08b805df344225845f80ef54ce/behavior
URL, IP address, domain or file hash
mitre
1/3
Sign in
Sign up

VirusTotal Jujubox 0 0 0 0 0 0 — Zenbox 0 5 0 0 1 1

Activity Summary — Download Artifacts, Full Reports, Help

Detections	Mitre Signatures	IDS Rules	Sigma Rules	Dropped Files	Network comms
NOT FOUND	9 INFO	NOT FOUND	NOT FOUND	130 OTHER 1 TEXT	4 DNS 45 IP

Behavior Tags

checks-user-input, idle, runtime-modules

MITRE ATT&CK Tactics and Techniques

- Privilege Escalation TA0004
- Defense Evasion TA0005
- Credential Access TA0006
- Discovery TA0007
- Collection TA0009
- Command and Control TA0011

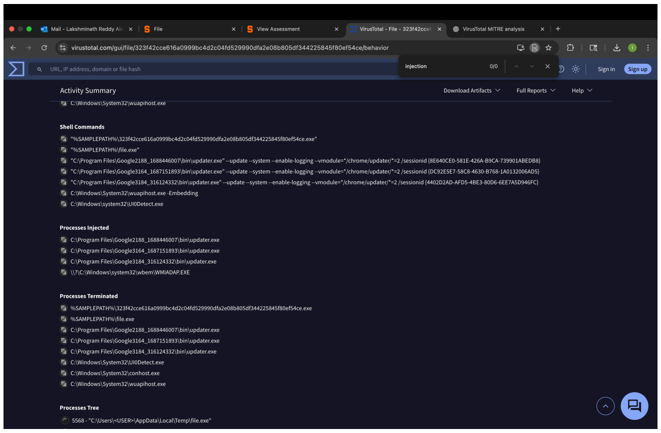
Malware Behavior Catalog Tree

- Anti-Behavioral Analysis OB0001
- Anti-Static Analysis OB0002
- Defense Evasion OB0006
- Communication OC0006

Capabilities

3. In the same behavior tab, I can see below process inhjected

Processes Injected
C:\Program Files\Google2188_1688446007\bin\updater.exe
C:\Program Files\Google3164_1687151893\bin\updater.exe
C:\Program Files\Google3184_316124332\bin\updater.exe
\\?\C:\Windows\system32\wbem\WMIADAP.EXE


Mail - Lakshminath Reddy Ala
File
View Assessment
VirusTotal - File - 323f42cce6
VirusTotal MITRE analysis
virustotal.com/gui/file/323f42cce616a0999bc4d2c04fd529990dfa2e08b805df344225845f80ef54ce/behavior
URL, IP address, domain or file hash
injection
0/0
Sign in
Sign up

Activity Summary — Download Artifacts, Full Reports, Help

```
C:\Windows\System32\wuapihost.exe

Shell Commands
"%SAMPLEPATH%\323f42cce616a0999bc4d2c04fd529990dfa2e08b805df344225845f80ef54ce.exe"
"%SAMPLEPATH%\file.exe"
"C:\Program Files\Google2188_1688446007\bin\updater.exe" --update --system --enable-logging --vmodule=*/chrome/updater/*=2 /sessionid {8E640CE0-581E-426A-B9CA-739901ABEDB8}
"C:\Program Files\Google3164_1687151893\bin\updater.exe" --update --system --enable-logging --vmodule=*/chrome/updater/*=2 /sessionid {DC92E5E7-58C8-4630-B768-1A0132006AD5}
"C:\Program Files\Google3184_316124332\bin\updater.exe" --update --system --enable-logging --vmodule=*/chrome/updater/*=2 /sessionid {4402D2AD-AFD5-4BE3-80D6-6EE7A5D946FC}
C:\Windows\System32\wuapihost.exe -Embedding
C:\Windows\system32\UI0Detect.exe

Processes Injected
C:\Program Files\Google2188_1688446007\bin\updater.exe
C:\Program Files\Google3164_1687151893\bin\updater.exe
C:\Program Files\Google3184_316124332\bin\updater.exe
\\?\C:\Windows\system32\wbem\WMIADAP.EXE

Processes Terminated
%SAMPLEPATH%\323f42cce616a0999bc4d2c04fd529990dfa2e08b805df344225845f80ef54ce.exe
%SAMPLEPATH%\file.exe
C:\Program Files\Google2188_1688446007\bin\updater.exe
C:\Program Files\Google3164_1687151893\bin\updater.exe
C:\Program Files\Google3184_316124332\bin\updater.exe
C:\Windows\System32\UI0Detect.exe
C:\Windows\System32\conhost.exe
C:\Windows\System32\wuapihost.exe

Processes Tree
5568 - "C:\Users\<USER>\AppData\Local\Temp\file.exe"
```