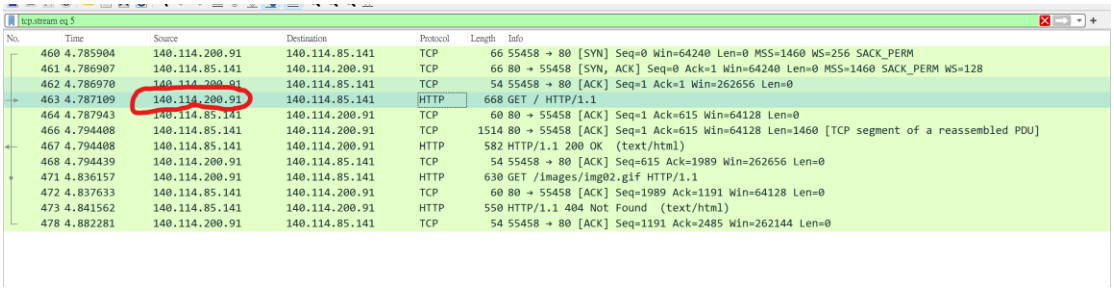
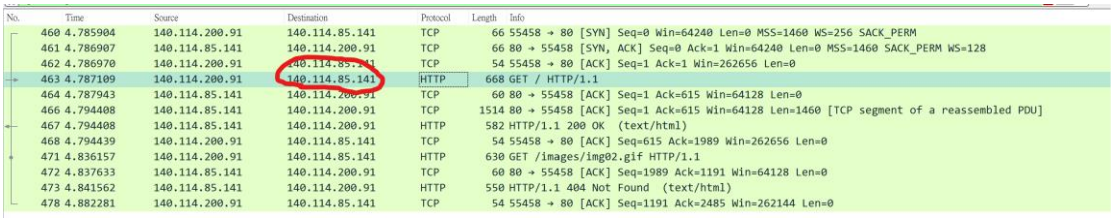
(1)HTTP

(a)140.114.200.91



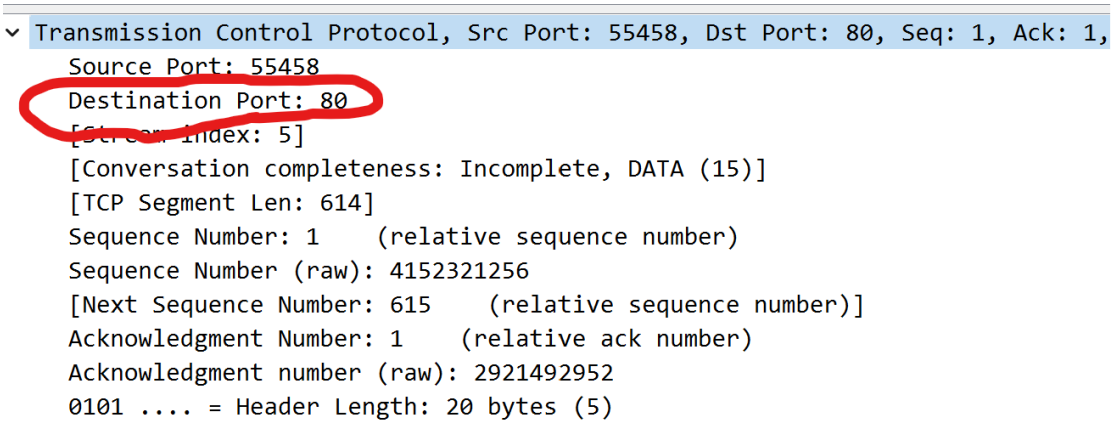
No.	Time	Source	Destination	Protocol	Length	Info
460	4.785904	140.114.200.91	140.114.85.141	TCP	66	55458 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
461	4.786907	140.114.85.141	140.114.200.91	TCP	66	80 → 55458 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
462	4.786970	140.114.200.91	140.114.85.141	TCP	54	55458 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
463	4.787109	140.114.200.91	140.114.85.141	HTTP	668	GET / HTTP/1.1
464	4.787943	140.114.85.141	140.114.200.91	TCP	60	80 → 55458 [ACK] Seq=1 Ack=615 Win=64128 Len=0
466	4.794408	140.114.85.141	140.114.200.91	TCP	1514	80 → 55458 [ACK] Seq=1 Ack=615 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
467	4.794408	140.114.85.141	140.114.200.91	HTTP	582	HTTP/1.1 200 OK (text/html)
468	4.794439	140.114.200.91	140.114.85.141	TCP	54	55458 → 80 [ACK] Seq=615 Ack=1989 Win=262656 Len=0
471	4.836157	140.114.200.91	140.114.85.141	HTTP	630	GET /images/img02.gif HTTP/1.1
472	4.837633	140.114.85.141	140.114.200.91	TCP	60	80 → 55458 [ACK] Seq=1989 Ack=1191 Win=64128 Len=0
473	4.841562	140.114.85.141	140.114.200.91	HTTP	550	HTTP/1.1 404 Not Found (text/html)
478	4.882281	140.114.200.91	140.114.85.141	TCP	54	55458 → 80 [ACK] Seq=1191 Ack=2485 Win=262144 Len=0

(b) 140.114.85.141



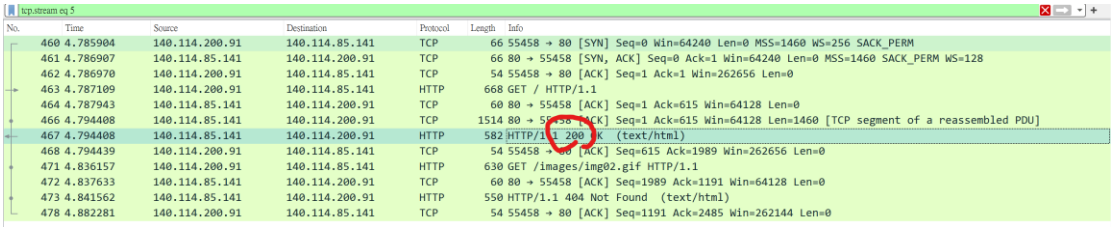
No.	Time	Source	Destination	Protocol	Length	Info
460	4.785904	140.114.200.91	140.114.85.141	TCP	66	55458 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
461	4.786907	140.114.85.141	140.114.200.91	TCP	66	80 → 55458 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
462	4.786970	140.114.200.91	140.114.85.141	TCP	54	55458 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
463	4.787109	140.114.200.91	140.114.85.141	HTTP	668	GET / HTTP/1.1
464	4.787943	140.114.85.141	140.114.200.91	TCP	60	80 → 55458 [ACK] Seq=1 Ack=615 Win=64128 Len=0
466	4.794408	140.114.85.141	140.114.200.91	TCP	1514	80 → 55458 [ACK] Seq=1 Ack=615 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
467	4.794408	140.114.85.141	140.114.200.91	HTTP	582	HTTP/1.1 200 OK (text/html)
468	4.794439	140.114.200.91	140.114.85.141	TCP	54	55458 → 80 [ACK] Seq=615 Ack=1989 Win=262656 Len=0
471	4.836157	140.114.200.91	140.114.85.141	HTTP	630	GET /images/img02.gif HTTP/1.1
472	4.837633	140.114.85.141	140.114.200.91	TCP	60	80 → 55458 [ACK] Seq=1989 Ack=1191 Win=64128 Len=0
473	4.841562	140.114.85.141	140.114.200.91	HTTP	550	HTTP/1.1 404 Not Found (text/html)
478	4.882281	140.114.200.91	140.114.85.141	TCP	54	55458 → 80 [ACK] Seq=1191 Ack=2485 Win=262144 Len=0

(c) 80



```
Transmission Control Protocol, Src Port: 55458, Dst Port: 80, Seq: 1, Ack: 1,
    Source Port: 55458
    Destination Port: 80
    [Stream index: 5]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 614]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 4152321256
    [Next Sequence Number: 615    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2921492952
    0101 .... = Header Length: 20 bytes (5)
```

(d) 200，request succeeded，requested object later in this massaeg



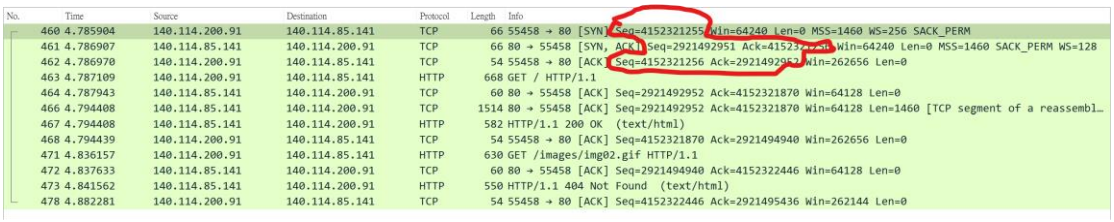
No.	Time	Source	Destination	Protocol	Length	Info
460	4.785904	140.114.200.91	140.114.85.141	TCP	66	55458 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
461	4.786907	140.114.85.141	140.114.200.91	TCP	66	80 → 55458 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
462	4.786970	140.114.200.91	140.114.85.141	TCP	54	55458 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
463	4.787109	140.114.200.91	140.114.85.141	HTTP	668	GET / HTTP/1.1
464	4.787943	140.114.85.141	140.114.200.91	TCP	60	80 → 55458 [ACK] Seq=1 Ack=615 Win=64128 Len=0
466	4.794408	140.114.85.141	140.114.200.91	TCP	1514	80 → 55458 [ACK] Seq=1 Ack=615 Win=64128 Len=1460 [TCP segment of a reassembled PDU]
467	4.794408	140.114.85.141	140.114.200.91	HTTP	582	HTTP/1.1 200 OK (text/html)
468	4.794439	140.114.200.91	140.114.85.141	TCP	54	55458 → 80 [ACK] Seq=615 Ack=1989 Win=262656 Len=0
471	4.836157	140.114.200.91	140.114.85.141	HTTP	630	GET /images/img02.gif HTTP/1.1
472	4.837633	140.114.85.141	140.114.200.91	TCP	60	80 → 55458 [ACK] Seq=1989 Ack=1191 Win=64128 Len=0
473	4.841562	140.114.85.141	140.114.200.91	HTTP	550	HTTP/1.1 404 Not Found (text/html)
478	4.882281	140.114.200.91	140.114.85.141	TCP	54	55458 → 80 [ACK] Seq=1191 Ack=2485 Win=262144 Len=0

(e)

1: Client → Server SEQ number (raw) =4152323255

2: Server → Client SEQ number (raw) =2921492951，ACK number (raw) =4152321256

3: Client → Server SEQ number (raw) =4152321256，ACK number (raw) =2921492952



No.	Time	Source	Destination	Protocol	Length	Info
460	4.785904	140.114.200.91	140.114.85.141	TCP	66	55458 → 80 [SYN] Seq=4152321255 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
461	4.786907	140.114.85.141	140.114.200.91	TCP	66	80 → 55458 [SYN, ACK] Seq=2921492951 Ack=4152321256 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
462	4.786970	140.114.200.91	140.114.85.141	TCP	54	55458 → 80 [ACK] Seq=4152321256 Ack=2921492952 Win=262656 Len=0
463	4.787109	140.114.200.91	140.114.85.141	HTTP	668	GET / HTTP/1.1
464	4.787943	140.114.85.141	140.114.200.91	TCP	60	80 → 55458 [ACK] Seq=2921492952 Ack=4152321870 Win=64128 Len=0
466	4.794408	140.114.85.141	140.114.200.91	TCP	1514	80 → 55458 [ACK] Seq=2921492952 Ack=4152321870 Win=64128 Len=1460 [TCP segment of a reassembl…
467	4.794408	140.114.85.141	140.114.200.91	HTTP	582	HTTP/1.1 200 OK (text/html)
468	4.794439	140.114.200.91	140.114.85.141	TCP	54	55458 → 80 [ACK] Seq=4152321870 Ack=2921494940 Win=262656 Len=0
471	4.836157	140.114.200.91	140.114.85.141	HTTP	630	GET /images/img02.gif HTTP/1.1
472	4.837633	140.114.85.141	140.114.200.91	TCP	60	80 → 55458 [ACK] Seq=2921494940 Ack=4152322446 Win=64128 Len=0
473	4.841562	140.114.85.141	140.114.200.91	HTTP	550	HTTP/1.1 404 Not Found (text/html)
478	4.882281	140.114.200.91	140.114.85.141	TCP	54	55458 → 80 [ACK] Seq=4152322446 Ack=2921495436 Win=262144 Len=0

(f) 1: Client → Server SEQ number = x

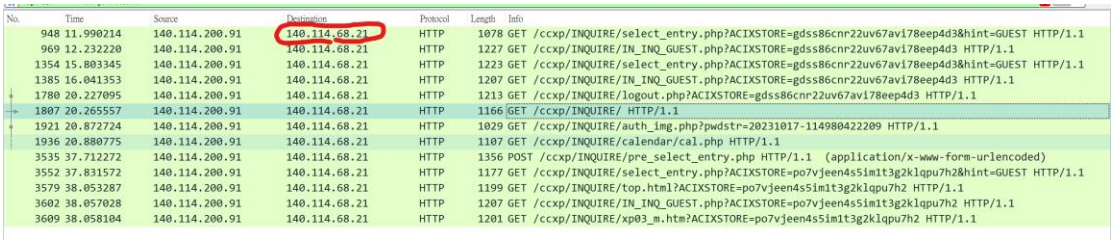
2: Server → Client SEQ number = y , ACK number = x+1

3: Client → Server SEQ number = x+1 , ACK number =y+1

(2)HTTPS

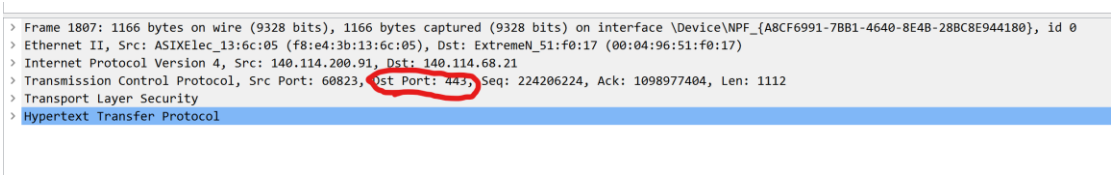
(a) 因為 HTTPS 使用加密來保護在客戶端和伺服器之間發送的資訊，HTTPS 使用 TLS 來加密資料。

(b) 140.114.68.21



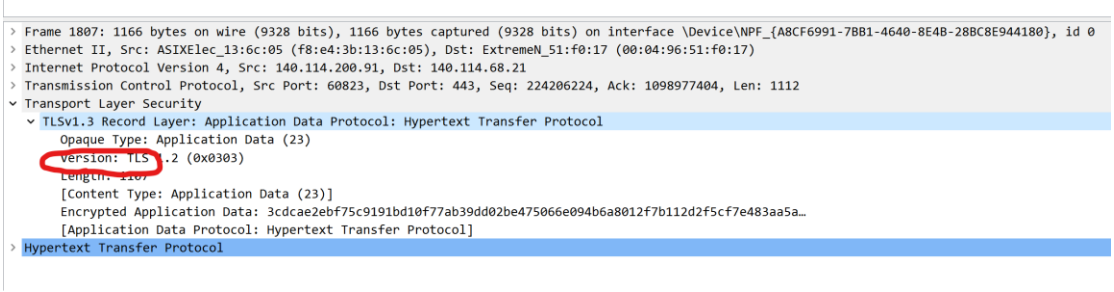
No.	Time	Source	Destination	Protocol	Length	Info
948	11.990214	140.114.200.91	140.114.68.21	HTTP	1078	GET /ccxp/INQUIRE/select_entry.php?ACIXSTORE=gdss86cnr22uv67avi78eep4d3&hint=GUEST HTTP/1.1
969	12.232220	140.114.200.91	140.114.68.21	HTTP	1227	GET /ccxp/INQUIRE/IN_INQ_GUEST.php?ACIXSTORE=gdss86cnr22uv67avi78eep4d3 HTTP/1.1
1354	15.803345	140.114.200.91	140.114.68.21	HTTP	1223	GET /ccxp/INQUIRE/select_entry.php?ACIXSTORE=gdss86cnr22uv67avi78eep4d3&hint=GUEST HTTP/1.1
1385	16.041353	140.114.200.91	140.114.68.21	HTTP	1207	GET /ccxp/INQUIRE/IN_INQ_GUEST.php?ACIXSTORE=gdss86cnr22uv67avi78eep4d3 HTTP/1.1
1780	20.227095	140.114.200.91	140.114.68.21	HTTP	1213	GET /ccxp/INQUIRE/logout.php?ACIXSTORE=gdss86cnr22uv67avi78eep4d3 HTTP/1.1
1807	20.265557	140.114.200.91	140.114.68.21	HTTP	1166	GET /ccxp/INQUIRE/ HTTP/1.1
1921	20.872724	140.114.200.91	140.114.68.21	HTTP	1029	GET /ccxp/INQUIRE/auth_img.php?pwdstr=20231017-114980422209 HTTP/1.1
1936	20.880775	140.114.200.91	140.114.68.21	HTTP	1107	GET /ccxp/INQUIRE/calendar/cal.php HTTP/1.1
3535	37.712272	140.114.200.91	140.114.68.21	HTTP	1356	POST /ccxp/INQUIRE/pre_select_entry.php HTTP/1.1 (application/x-www-form-urlencoded)
3552	37.831572	140.114.200.91	140.114.68.21	HTTP	1177	GET /ccxp/INQUIRE/select_entry.php?ACIXSTORE=po7vjeen4s5im1t3g2klqpu7h2&hint=GUEST HTTP/1.1
3579	38.053287	140.114.200.91	140.114.68.21	HTTP	1199	GET /ccxp/INQUIRE/top.html?ACIXSTORE=po7vjeen4s5im1t3g2klqpu7h2 HTTP/1.1
3602	38.057028	140.114.200.91	140.114.68.21	HTTP	1207	GET /ccxp/INQUIRE/IN_INQ_GUEST.php?ACIXSTORE=po7vjeen4s5im1t3g2klqpu7h2 HTTP/1.1
3609	38.058104	140.114.200.91	140.114.68.21	HTTP	1201	GET /ccxp/INQUIRE/xp03_m.htm?ACIXSTORE=po7vjeen4s5im1t3g2klqpu7h2 HTTP/1.1

(c) 443



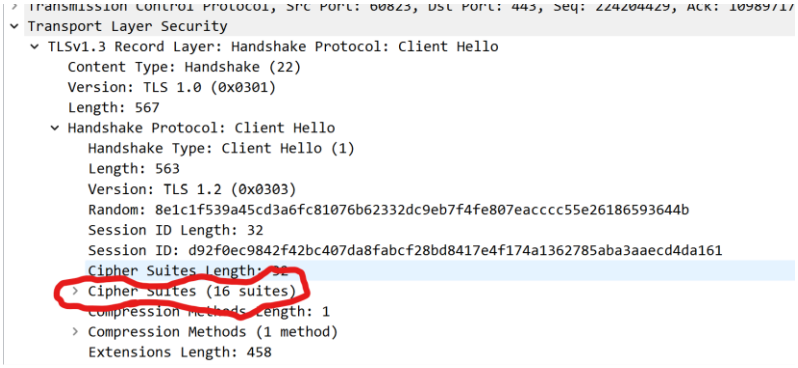
```
> Frame 1807: 1166 bytes on wire (9328 bits), 1166 bytes captured (9328 bits) on interface \Device\NPF_{A8CF6991-7BB1-4640-8E4B-28BC8E944180}, id 0
> Ethernet II, Src: ASIXElec_13:6c:05 (f8:e4:3b:13:6c:05), Dst: ExtremeN_51:f0:17 (00:04:96:51:f0:17)
> Internet Protocol Version 4, Src: 140.114.200.91, Dst: 140.114.68.21
> Transmission Control Protocol, Src Port: 60823, Dst Port: 443, Seq: 224206224, Ack: 1098977404, Len: 1112
> Transport Layer Security
> Hypertext Transfer Protocol
```

(d) TLS



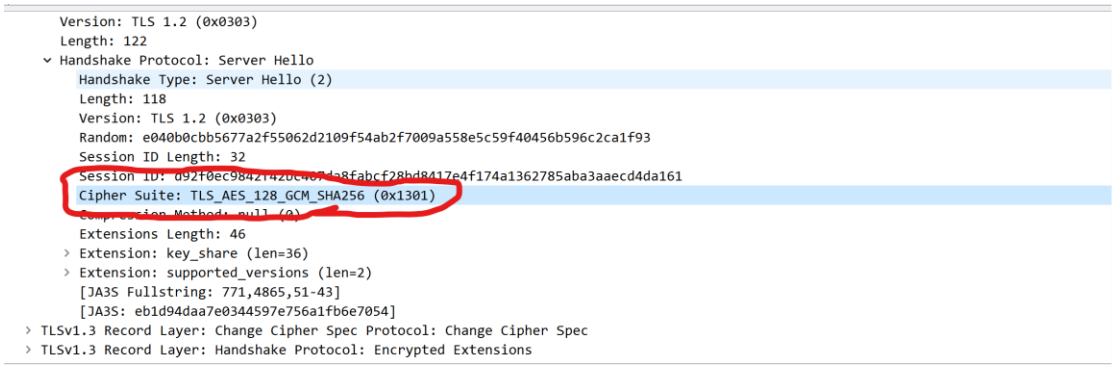
```
> Frame 1807: 1166 bytes on wire (9328 bits), 1166 bytes captured (9328 bits) on interface \Device\NPF_{A8CF6991-7BB1-4640-8E4B-28BC8E944180}, id 0
> Ethernet II, Src: ASIXElec_13:6c:05 (f8:e4:3b:13:6c:05), Dst: ExtremeN_51:f0:17 (00:04:96:51:f0:17)
> Internet Protocol Version 4, Src: 140.114.200.91, Dst: 140.114.68.21
> Transmission Control Protocol, Src Port: 60823, Dst Port: 443, Seq: 224206224, Ack: 1098977404, Len: 1112
v Transport Layer Security
  v TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
      Opaque Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 1107
      [Content Type: Application Data (23)]
      Encrypted Application Data: 3cdcae2ebf75c9191bd10f77ab39dd02be475066e094b6a8012f7b112d2f5cf7e483aa5a…
      [Application Data Protocol: Hypertext Transfer Protocol]
> Hypertext Transfer Protocol
```

(e)16 suites



```
Transmission Control Protocol, Src Port: 60823, Dst Port: 443, Seq: 224204429, Ack: 1098971
v Transport Layer Security
  v TLSv1.3 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 567
    v Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 563
        Version: TLS 1.2 (0x0303)
        Random: 8e1c1f539a45cd3a6fc81076b62332dc9eb7f4fe807eacccc55e26186593644b
        Session ID Length: 32
        Session ID: d92f0ec9842f42bc407da8fabcf28bd8417e4f174a1362785aba3aaecd4da161
        Cipher Suites Length: 32
      > Cipher Suites (16 suites)
        Compression Methods Length: 1
      > Compression Methods (1 method)
        Extensions Length: 458
```

(f) TLS_AES_GCM_SHA256(0x1301)



(g)