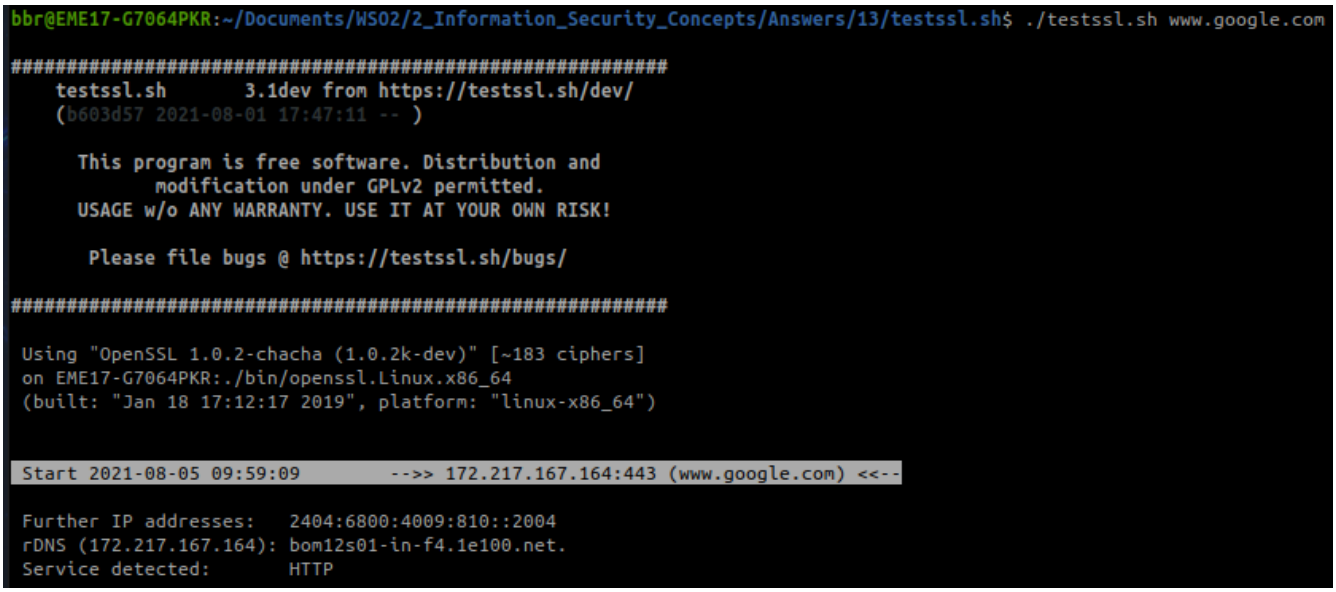
13. **Test SSL configuration using testssl.sh**

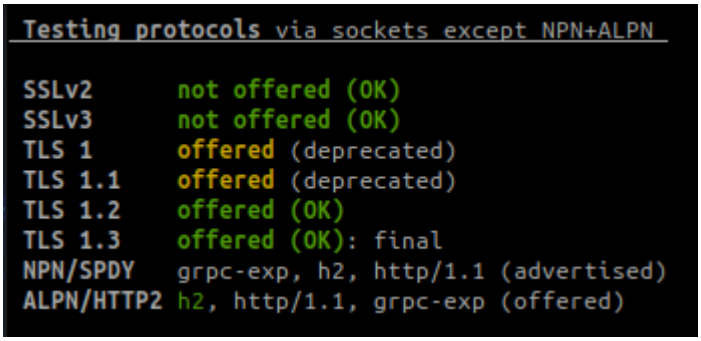
To perform a full test on the domain execute the following command. Then it will start the test and will take a little time to complete.

```
# ./testssl.sh www.google.com
```

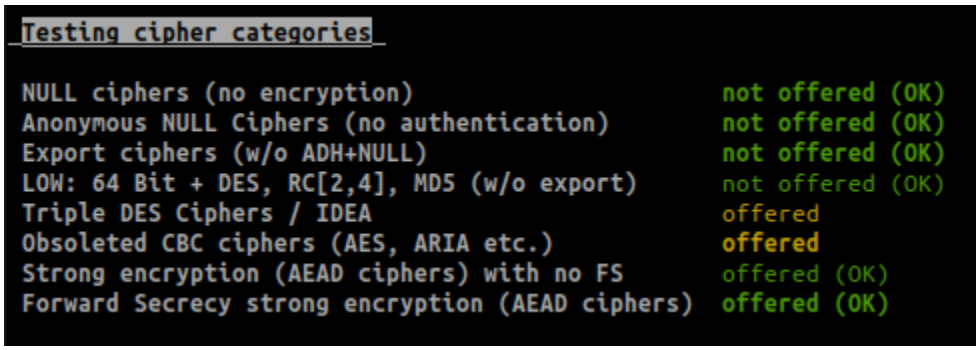


This test can be executed in single check options, single check as <options>

Testing protocols (-p) # ./testssl.sh **-p** www.google.com



Testing cipher categories # ./testssl.sh -s www.google.com



Testing server's cipher preferences # ./testssl.sh -P www.google.com

```
 Testing server's cipher preferences

 Has server cipher order?     yes (OK) -- only for < TLS 1.3
 Negotiated protocol          TLSv1.3
 Negotiated cipher            TLS_AES_256_GCM_SHA384, 253 bit ECDH (X25519)
 Cipher per protocol

Hexcode  Cipher Suite Name (OpenSSL)       KeyExch.   Encryption  Bits     Cipher Suite Name (IANA/RFC)
-----------------------------------------------------------------------------------------------------------------------------
SSLv2
 -
SSLv3
 -
TLSv1 (server order)
 xc009   ECDHE-ECDSA-AES128-SHA           ECDH 256   AES         128      TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
 xc00a   ECDHE-ECDSA-AES256-SHA           ECDH 256   AES         256      TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
 xc013   ECDHE-RSA-AES128-SHA             ECDH 256   AES         128      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
 xc014   ECDHE-RSA-AES256-SHA             ECDH 256   AES         256      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
 x2f     AES128-SHA                       RSA        AES         128      TLS_RSA_WITH_AES_128_CBC_SHA
 x35     AES256-SHA                       RSA        AES         256      TLS_RSA_WITH_AES_256_CBC_SHA
 x0a     DES-CBC3-SHA                     RSA        3DES        168      TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLSv1.1 (server order)
 xc009   ECDHE-ECDSA-AES128-SHA           ECDH 256   AES         128      TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
 xc00a   ECDHE-ECDSA-AES256-SHA           ECDH 256   AES         256      TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
 xc013   ECDHE-RSA-AES128-SHA             ECDH 256   AES         128      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
 xc014   ECDHE-RSA-AES256-SHA             ECDH 256   AES         256      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
 x2f     AES128-SHA                       RSA        AES         128      TLS_RSA_WITH_AES_128_CBC_SHA
 x35     AES256-SHA                       RSA        AES         256      TLS_RSA_WITH_AES_256_CBC_SHA
 x0a     DES-CBC3-SHA                     RSA        3DES        168      TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLSv1.2 (server order)
 xcca9   ECDHE-ECDSA-CHACHA20-POLY1305    ECDH 253   ChaCha20    256      TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
 xc02b   ECDHE-ECDSA-AES128-GCM-SHA256    ECDH 253   AESGCM      128      TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
 xc02c   ECDHE-ECDSA-AES256-GCM-SHA384    ECDH 253   AESGCM      256      TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
 xc009   ECDHE-ECDSA-AES128-SHA           ECDH 253   AES         128      TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
 xc00a   ECDHE-ECDSA-AES256-SHA           ECDH 253   AES         256      TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
 xcca8   ECDHE-RSA-CHACHA20-POLY1305      ECDH 253   ChaCha20    256      TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
 xc02f   ECDHE-RSA-AES128-GCM-SHA256      ECDH 253   AESGCM      128      TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 xc030   ECDHE-RSA-AES256-GCM-SHA384      ECDH 253   AESGCM      256      TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 xc013   ECDHE-RSA-AES128-SHA             ECDH 253   AES         128      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
 xc014   ECDHE-RSA-AES256-SHA             ECDH 253   AES         256      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
 x9c     AES128-GCM-SHA256                RSA        AESGCM      128      TLS_RSA_WITH_AES_128_GCM_SHA256
 x9d     AES256-GCM-SHA384                RSA        AESGCM      256      TLS_RSA_WITH_AES_256_GCM_SHA384
 x2f     AES128-SHA                       RSA        AES         128      TLS_RSA_WITH_AES_128_CBC_SHA
 x35     AES256-SHA                       RSA        AES         256      TLS_RSA_WITH_AES_256_CBC_SHA
 x0a     DES-CBC3-SHA                     RSA        3DES        168      TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLSv1.3 (no server order, thus listed by strength)
 x1302   TLS_AES_256_GCM_SHA384           ECDH 253   AESGCM      256      TLS_AES_256_GCM_SHA384
 x1303   TLS_CHACHA20_POLY1305_SHA256     ECDH 253   ChaCha20    256      TLS_CHACHA20_POLY1305_SHA256
 x1301   TLS_AES_128_GCM_SHA256           ECDH 253   AESGCM      128      TLS_AES_128_GCM_SHA256
```

Testing vulnerabilities # ./testssl.sh -U www.google.com

```
 Testing vulnerabilities

 Heartbleed (CVE-2014-0160)                not vulnerable (OK), no heartbeat extension
 CCS (CVE-2014-0224)                       not vulnerable (OK)
 Ticketbleed (CVE-2016-9244), experiment.  not vulnerable (OK)
 ROBOT                                     not vulnerable (OK)
 Secure Renegotiation (RFC 5746)           supported (OK)
 Secure Client-Initiated Renegotiation     not vulnerable (OK)
 CRIME, TLS (CVE-2012-4929)                not vulnerable (OK)
 BREACH (CVE-2013-3587)                    potentially NOT ok, "gzip" HTTP compression detected. - only supplied "/" tested
                                           Can be ignored for static pages or if no secrets in the page
 POODLE, SSL (CVE-2014-3566)               not vulnerable (OK), no SSLv3 support
 TLS_FALLBACK_SCSV (RFC 7507)              Downgrade attack prevention supported (OK)
 SWEET32 (CVE-2016-2183, CVE-2016-6329)    VULNERABLE, uses 64 bit block ciphers
 FREAK (CVE-2015-0204)                     not vulnerable (OK)
 DROWN (CVE-2016-0800, CVE-2016-0703)      not vulnerable on this host and port (OK)
                                           make sure you don't use this certificate elsewhere with SSLv2 enabled services
                                           https://censys.io/ipv4?q=7E14A04D78778A6BFC2DD49D32E346BD922D0D72E87D0E5C47037AC70B6EBAB7 could help you to find out
 LOGJAM (CVE-2015-4000), experimental      not vulnerable (OK): no DH EXPORT ciphers, no DH key detected with <= TLS 1.2
 BEAST (CVE-2011-3389)                     TLS1: ECDHE-ECDSA-AES128-SHA ECDHE-ECDSA-AES256-SHA ECDHE-RSA-AES128-SHA ECDHE-RSA-AES256-SHA AES128-SHA AES256-SHA DES-CBC3-SHA
                                           VULNERABLE -- but also supports higher protocols  TLSv1.1 TLSv1.2 (likely mitigated)
 LUCKY13 (CVE-2013-0169), experimental     potentially VULNERABLE, uses cipher block chaining (CBC) ciphers with TLS. Check patches
 Winshock (CVE-2014-6321), experimental    not vulnerable (OK)
 RC4 (CVE-2013-2566, CVE-2015-2808)        no RC4 ciphers detected (OK)
```

Testing server defaults (Server Hello)

```
Testing server defaults (Server Hello)

TLS extensions (standard)    "renegotiation info/#65281" "EC point formats/#11" "session ticket/#35" "next protocol/#13172" "key share/#51" "supported versions/#43"
                             "extended master secret/#23" "application layer protocol negotiation/#16"
Session Ticket RFC 5077 hint 100799 seconds but: FS requires session ticket keys to be rotated < daily !
SSL Session ID support       yes
Session Resumption           Tickets: yes, ID: yes
TLS clock skew               -1 sec from localtime
Client Authentication        none

 Server Certificate #1
  Signature Algorithm          SHA256 with RSA
  Server key size              RSA 2048 bits (exponent is 65537)
  Server key usage             Digital Signature, Key Encipherment
  Server extended key usage    TLS Web Server Authentication
  Serial / Fingerprints        CDF432A1C8ED30680A00000000EB6102 / SHA1 195AB4E0902BE7F91A053C8213BD213D92D36836
                               SHA256 7E14A04D78778A6BFC2DD49D32E346BD922D0D72E87D0E5C47037AC70B6EBAB7
  Common Name (CN)             www.google.com
  subjectAltName (SAN)         www.google.com
  Trust (hostname)             Ok via SAN and CN (same w/o SNI)
  Chain of trust               Ok
  EV cert (experimental)       no
  Certificate Validity (UTC)   expires < 60 days (45) (2021-06-28 04:12 --> 2021-09-20 04:12)
  ETS/"eTLS", visibility info  not present
  Certificate Revocation List  http://crls.pki.goog/gts1c3/QqFxbi9M48c.crl
  OCSP URI                     http://ocsp.pki.goog/gts1c3
  OCSP stapling                not offered
  OCSP must staple extension   --
  DNS CAA RR (experimental)    available - please check for match with "Issuer" below: issue=pki.goog
  Certificate Transparency     yes (certificate extension)
  Certificates provided        3
  Issuer                       GTS CA 1C3 (Google Trust Services LLC from US)
  Intermediate cert validity   #1: ok > 40 days (2027-09-30 00:00). GTS CA 1C3 <-- GTS Root R1
                                 #2: ok > 40 days (2028-01-28 00:00). GTS Root R1 <-- GlobalSign Root CA
  Intermediate Bad OCSP (exp.) Ok
```

```
Server Certificate #2
  Signature Algorithm          SHA256 with RSA
  Server key size              EC 256 bits (curve P-256)
  Server key usage             Digital Signature
  Server extended key usage    TLS Web Server Authentication
  Serial / Fingerprints        12D4D6BAD37B1DD10A00000000EB6108 / SHA1 66796D0D5106CED07B16084EC8DA536DD7C0D010
                               SHA256 C8C5DCF3042EEE9AB9BAC528F0A12B3178F70643B86507A0C30FC98FDA48EA8E
  Common Name (CN)             www.google.com
  subjectAltName (SAN)         www.google.com
  Trust (hostname)             Ok via SAN and CN (same w/o SNI)
  Chain of trust               Ok
  EV cert (experimental)       no
  Certificate Validity (UTC)   expires < 60 days (45) (2021-06-28 04:12 --> 2021-09-20 04:12)
  ETS/"eTLS", visibility info  not present
  Certificate Revocation List  http://crls.pki.goog/gts1c3/fVJxbV-Ktmk.crl
  OCSP URI                     http://ocsp.pki.goog/gts1c3
  OCSP stapling                not offered
  OCSP must staple extension   --
  DNS CAA RR (experimental)    available - please check for match with "Issuer" below: issue=pki.goog
  Certificate Transparency     yes (certificate extension)
  Certificates provided        3
  Issuer                       GTS CA 1C3 (Google Trust Services LLC from US)
  Intermediate cert validity   #1: ok > 40 days (2027-09-30 00:00). GTS CA 1C3 <-- GTS Root R1
                                 #2: ok > 40 days (2028-01-28 00:00). GTS Root R1 <-- GlobalSign Root CA
  Intermediate Bad OCSP (exp.) Ok
```

Tests HSTS, HPKP, server/app banner, security headers, cookie, reverse proxy, IPv4 address # ./testssl.sh -h www.google.com

```
Testing HTTP header response @ "/"

HTTP Status Code             200 OK
HTTP clock skew              0 sec from localtime
Strict Transport Security    not offered
Public Key Pinning           --
Server banner                gws
Application banner           --
Cookie(s)                    2 issued: 1/2 secure, 1/2 HttpOnly
Security headers             X-Frame-Options: SAMEORIGIN
                             X-XSS-Protection: 0
                             Cache-Control: private, max-age=0
Reverse Proxy banner         --
```

Test client simulations, see which client negotiates with cipher and protocol

./testssl.sh -c www.google.com

```
 Running client simulations (HTTP) via sockets

 Browser                    Protocol  Cipher Suite Name (OpenSSL)       Forward Secrecy
--------------------------------------------------------------------------------------------
 Android 4.4.2              TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     256 bit ECDH (P-256)
 Android 5.0.0              TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     256 bit ECDH (P-256)
 Android 6.0                TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     256 bit ECDH (P-256)
 Android 7.0 (native)       TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     256 bit ECDH (P-256)
 Android 8.1 (native)       TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     253 bit ECDH (X25519)
 Android 9.0 (native)       TLSv1.3   TLS_AES_128_GCM_SHA256            253 bit ECDH (X25519)
 Android 10.0 (native)      TLSv1.3   TLS_AES_128_GCM_SHA256            253 bit ECDH (X25519)
 Chrome 74 (Win 10)         TLSv1.3   TLS_AES_128_GCM_SHA256            253 bit ECDH (X25519)
 Chrome 79 (Win 10)         TLSv1.3   TLS_AES_128_GCM_SHA256            253 bit ECDH (X25519)
 Firefox 66 (Win 8.1/10)    TLSv1.3   TLS_AES_128_GCM_SHA256            253 bit ECDH (X25519)
 Firefox 71 (Win 10)        TLSv1.3   TLS_AES_128_GCM_SHA256            253 bit ECDH (X25519)
 IE 6 XP                    No connection
 IE 8 Win 7                 TLSv1.0   ECDHE-ECDSA-AES128-SHA            256 bit ECDH (P-256)
 IE 8 XP                    TLSv1.0   DES-CBC3-SHA                      No FS
 IE 11 Win 7                TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     256 bit ECDH (P-256)
 IE 11 Win 8.1              TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     256 bit ECDH (P-256)
 IE 11 Win Phone 8.1        TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     256 bit ECDH (P-256)
 IE 11 Win 10               TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     256 bit ECDH (P-256)
 Edge 15 Win 10             TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     253 bit ECDH (X25519)
 Edge 17 (Win 10)           TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     253 bit ECDH (X25519)
 Opera 66 (Win 10)          TLSv1.3   TLS_AES_128_GCM_SHA256            253 bit ECDH (X25519)
 Safari 9 iOS 9             TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     256 bit ECDH (P-256)
 Safari 9 OS X 10.11        TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     256 bit ECDH (P-256)
 Safari 10 OS X 10.12       TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     256 bit ECDH (P-256)
 Safari 12.1 (iOS 12.2)     TLSv1.3   TLS_CHACHA20_POLY1305_SHA256      253 bit ECDH (X25519)
 Safari 13.0 (macOS 10.14.6) TLSv1.3  TLS_CHACHA20_POLY1305_SHA256      253 bit ECDH (X25519)
 Apple ATS 9 iOS 9          TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     256 bit ECDH (P-256)
 Java 6u45                  TLSv1.0   AES128-SHA                        No FS
 Java 7u25                  TLSv1.0   ECDHE-ECDSA-AES128-SHA            256 bit ECDH (P-256)
 Java 8u161                 TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     256 bit ECDH (P-256)
 Java 11.0.2 (OpenJDK)      TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     256 bit ECDH (P-256)
 Java 12.0.1 (OpenJDK)      TLSv1.3   TLS_AES_128_GCM_SHA256            256 bit ECDH (P-256)
 OpenSSL 1.0.2e             TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     256 bit ECDH (P-256)
 OpenSSL 1.1.0l (Debian)    TLSv1.2   ECDHE-ECDSA-CHACHA20-POLY1305     253 bit ECDH (X25519)
 OpenSSL 1.1.1d (Debian)    TLSv1.3   TLS_AES_256_GCM_SHA384            253 bit ECDH (X25519)
 Thunderbird (68.3)         TLSv1.3   TLS_AES_128_GCM_SHA256            253 bit ECDH (X25519)
```

Rating (experimental)

```
 Rating (experimental)

 Rating specs (not complete)  SSL Labs's 'SSL Server Rating Guide' (version 2009q from 2020-01-30)
 Specification documentation  https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide
 Protocol Support (weighted)  95 (28)
 Key Exchange     (weighted)  90 (27)
 Cipher Strength  (weighted)  90 (36)
 Final Score                  91
 Overall Grade                B
 Grade cap reasons            Grade capped to B. TLS 1.1 offered
                              Grade capped to B. TLS 1.0 offered
                              Grade capped to A. HSTS is not offered
```