

Praktikant: Wilhelm Görlitz

MatrikelNr: 751235

Praktikant: Simon Grimm

MatrikelNR: 750813

IT-Sicherheit Praktikum 4

a)

MAC: Source: CadmusCo_51:c9:65 (08:00:27:51:c9:65)

IP:

Source
10.0.2.15

b)

http						
No.	Time	Source	Destination	Protocol	Length	Info
18	2.497248	10.0.2.15	212.227.70.81	HTTP	376	GET / HTTP/1.1
Hypertext Transfer Protocol						
GET / HTTP/1.1\r\n						
Host: www.dieburg.de\r\n						
Source Port: 33686						
Destination Port: 80						

c)

No.	Time	Source	Destination	Protocol	Length	Info
18	2.497248	10.0.2.15	212.227.70.81	HTTP	376	GET / HTTP/1.1
43	2.593938	10.0.2.15	172.217.22.14	OCSP	491	Request
46	2.624731	172.217.22.14	10.0.2.15	OCSP	800	Response
127	4.980535	212.227.70.81	10.0.2.15	HTTP	60	HTTP/1.1 200 OK (text/html)
159	7.041598	10.0.2.15	134.119.24.29	HTTP	429	GET / HTTP/1.1
161	7.067707	134.119.24.29	10.0.2.15	HTTP	409	HTTP/1.1 302 Moved Temporarily (text/html)
184	7.202533	10.0.2.15	104.16.28.216	OCSP	511	Request
189	7.227683	104.16.28.216	10.0.2.15	OCSP	744	Response
274	7.748681	10.0.2.15	104.16.28.216	OCSP	511	Request
278	7.774389	104.16.28.216	10.0.2.15	OCSP	744	Response
316	9.057002	10.0.2.15	172.217.22.14	OCSP	491	Request
320	9.089318	172.217.22.14	10.0.2.15	OCSP	800	Response
2881	12.892498	10.0.2.15	212.227.70.81	HTTP	511	GET /index.php/kultur-topmenu-28 HTTP/1.1
2918	13.563536	212.227.70.81	10.0.2.15	HTTP	60	HTTP/1.1 200 OK (text/html)

Daten, die ausgetauscht werden:

Paket18: Anfrage an den Server

Paket127: Antwort des Servers: "Anfrage in Ordnung"

Paket2881: Request URL: /index.php/kultur-topmenu-28

Auf dieburg.de wurde die Schaltfläche "KULTUR" angeklickt und eine Anfrage an den Server geschickt.

Paket2918: Antwort des Servers: "Anfrage in Ordnung".

d)

No.	Time	Source	Destination	Protocol	Length	Info
→ 5	2.437665	10.0.2.15	10.0.2.3	DNS	74	Standard query 0xdd7f A www.dieburg.de

▼ Domain Name System (query)

[\[Response In: 9\]](#)

Transaction ID: 0xdd7f

► Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

▼ Queries

► www.dieburg.de: type A, class IN

No.	Time	Source	Destination	Protocol
→ 5	2.437665	10.0.2.15	10.0.2.3	DNS
6	2.437866	10.0.2.15	10.0.2.3	DNS
7	2.438160	10.0.2.15	10.0.2.3	DNS
8	2.438263	10.0.2.15	10.0.2.3	DNS
← 9	2.444278	10.0.2.3	10.0.2.15	DNS

Wireshark · Pack

► User Datagram Protocol, Src Port: 53, Dst Port: 12639

▼ Domain Name System (response)

[\[Request In: 5\]](#)

[Time: 0.006613000 seconds]

Transaction ID: 0xdd7f

► Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 1

Authority RRs: 0

Additional RRs: 0

▼ Queries

► www.dieburg.de: type A, class IN

▼ Answers

► www.dieburg.de: type A, class IN, addr 212.227.70.81

10	2.471001	10.0.2.3	10.0.2.15
11	2.471300	10.0.2.15	212.227.70.81

▶ Frame 10: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits) on interface 0
 ▶ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: 08:00:27:00:00:00
 ▶ Internet Protocol Version 4, Src: 10.0.2.3, Dst: 10.0.2.15
 ▶ User Datagram Protocol, Src Port: 53, Dst Port: 17534
 ▼ Domain Name System (response)
 [Request In: 6]
 [Time: 0.033135000 seconds]
 Transaction ID: 0x6ec9
 ▶ Flags: 0x8180 Standard query response, No error
 Questions: 1
 Answer RRs: 0
 Authority RRs: 1
 Additional RRs: 0
 ▼ Queries
 ▼ www.dieburg.de: type AAAA, class IN
 Name: www.dieburg.de
 [Name Length: 14]
 [Label Count: 3]
 Type: AAAA (IPv6 Address) (28)
 Class: IN (0x0001)
 ▼ Authoritative nameservers

e)

166	7.108691	10.0.2.15	134.119.24.29	TLSv1.2	254 Client Hello
-----	----------	-----------	---------------	---------	------------------

Die IP-Adresse 134.119.24.29 gehört zu www.wikipedia.de.

f)

▼ Cipher Suites (15 suites)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)

168	7.138955	134.119.24.29	10.0.2.15	TLSv1.2	1454	Server Hello
Wireshark · Packet 168 · m4						
Content Type: Handshake (22) Version: TLS 1.2 (0x0303) Length: 74 ▼ Handshake Protocol: Server Hello Handshake Type: Server Hello (2) Length: 70 Version: TLS 1.2 (0x0303) ▶ Random Session ID Length: 0 Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)						

Oben zeigt der Client welche Verschlüsselungen er zur Verfügung hat. Im unteren Bild sieht man welche Verschlüsselung gewählt wurde. Da die AES-128 mit SHA256 Verschlüsselung gewählt wurde, besteht eine sichere Verbindung zwischen Client und Server.

171	7.144040	10.0.2.15	134.119.24.29	TCP	54 50966-443 [ACK] Seq=201 Ack=3699 Win=37800 Len=0
172	7.144854	134.119.24.29	10.0.2.15	TLSv1.2	952 CertificateServer Key Exchange, Server Hello Done
173	7.144859	10.0.2.15	134.119.24.29	TCP	54 50966-443 [ACK] Seq=201 Ack=3699 Win=37800 Len=0

Length: 3267

- ▼ Handshake Protocol: Certificate
 - Handshake Type: Certificate (11)
 - Length: 3263
 - Certificates Length: 3260
 - ▼ Certificates (3260 bytes)
 - Certificate Length: 1257
 - ▶ Certificate: 308204e5308203cda0030201020212112155df723231885d... (id-at-commonName=www.wikipedia.de,id-at-organizationalUnitName=Domain Control Validated,id-at-organizationalUnitName=Domain Control Validated,id-at-organizationalUnitName=Domain Control Validated)
 - Certificate Length: 1105
 - ▶ Certificate: 3082044d30820335a003020102020b040000000001444ef0... (id-at-commonName=AlphaSSL CA - SHA256 - G2,id-at-organizationName=GlobalSign nv-sa,id-at-coun-)
 - Certificate Length: 889
 - ▶ Certificate: 308203753082025da003020102020b040000000001154b5a... (id-at-commonName=GlobalSign Root CA,id-at-organizationalUnitName=Root CA,id-at-organizationNa)

▶ Secure Sockets Layer

e)

Der Wikipedia-Server.