

به نام خدا

| | |
|--------------------------------|-------------------------------|
| ۹۷۲۳۱۰۰ | محمد مهدی هجرتی |
| راه اندازی سرویس های Web و FTP | آزمایشگاه شبکه - آزمایش چهارم |
| ۳۰ فروردین ۱۴۰۰ | استاد نقی زاده |

سوال ۱

آدرس پورت مبدا ۸۰ و پورت مقصد ۶۲۹۴۹ می باشد.
برای برقراری ارتباط، ابتدا یک Tcp handshake شکل می گیرد. سپس در صورت موفقیت آمیز بودن، به ترتیب آجکت های صفحه ی مورد نظر برای کلاینت فرستاده می شود.
در اینجا چون سرور بر روی سیستم خودمان اجرا شده است، با مراجعه به hosts آدرس سایت را تشخیص می دهد.

*Adapter for loopback traffic capture

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 0

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|-----------|-------------|----------|--------|--|
| 3 | 4.396884 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 62949 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1 |
| 4 | 4.396969 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 80 → 62949 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 ... |
| 5 | 4.397034 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 62949 → 80 [ACK] Seq=1 Ack=1 Win=2619648 Len=0 |
| 9 | 4.401923 | 127.0.0.1 | 127.0.0.1 | HTTP | 595 | GET / HTTP/1.1 |
| 10 | 4.401958 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 80 → 62949 [ACK] Seq=1 Ack=552 Win=2619648 Len=0 |
| 11 | 4.417589 | 127.0.0.1 | 127.0.0.1 | HTTP | 489 | HTTP/1.1 200 OK (text/html) |
| 12 | 4.417621 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 62949 → 80 [ACK] Seq=552 Ack=446 Win=2619136 Len=0 |
| 14 | 9.425100 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 80 → 62949 [FIN, ACK] Seq=446 Ack=552 Win=2619648 Len=0 |
| 15 | 9.425127 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 62949 → 80 [ACK] Seq=552 Ack=447 Win=2619136 Len=0 |

> Frame 9: 595 bytes on wire (4760 bits), 595 bytes captured (4760 bits) on interface \Device\NPF_{...}_Loopback, id 0

> Null/Loopback

> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

> Transmission Control Protocol, Src Port: 62949, Dst Port: 80, Seq: 1, Ack: 1, Len: 551

> Hypertext Transfer Protocol

<

0000 02 00 00 00 45 00 02 4f 5c 72 40 00 80 06 00 00E..0 \r@....

0010 7f 00 00 01 7f 00 00 01 f5 e5 00 50 6d 58 ff 15PmX..

0020 23 eb 58 72 50 18 27 f9 39 69 00 00 47 45 54 20 #.XrP..'. 9i..GET

0030 2f 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 / HTTP/1.1..Host

Family (null.family), 4 bytes

Packets: 15 · Displayed: 9 (60.0%) · Dropped: 0 (0.0%) Profile: Default

سوال ۲

مقدار connection، keep-alive می باشد.

نوع درخواست GET می باشد.

مقدار user-agent، به صورت زیر می باشد.

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.128 Safari/537.36\r\n

این مقدار بیانگر، مشخصات سیستم عامل، مرورگر و ... مربوط به کلاینت درخواست دهنده می باشد.

*Adapter for loopback traffic capture

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 0

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|-----------|-------------|----------|--------|--|
| 3 | 4.396884 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 62949 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1 |
| 4 | 4.396969 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 80 → 62949 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 ... |
| 5 | 4.397034 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 62949 → 80 [ACK] Seq=1 Ack=1 Win=2619648 Len=0 |
| 9 | 4.401923 | 127.0.0.1 | 127.0.0.1 | HTTP | 595 | GET / HTTP/1.1 |
| 10 | 4.401958 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 80 → 62949 [ACK] Seq=1 Ack=552 Win=2619648 Len=0 |
| 11 | 4.417500 | 127.0.0.1 | 127.0.0.1 | HTTP | 400 | HTTP/1.1 200 OK (text/html) |

▼ Hypertext Transfer Protocol

GET / HTTP/1.1\r\n

Host: m_hejrati1.com\r\n

Connection: keep-alive\r\n

Upgrade-Insecure-Requests: 1\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.128 Safari/537.36\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9\r\n

Accept-Encoding: gzip, deflate\r\n

Accept-Language: en-US,en-GB;q=0.9,en;q=0.8,fa-IR;q=0.7,fa;q=0.6\r\n

If-None-Match: "89-5c053a3a5bc42"\r\n

If-Modified-Since: Mon, 19 Apr 2021 13:52:23 GMT\r\n

\r\n

0000 02 00 00 00 45 00 02 4f 5c 72 40 00 80 06 00 00E..O \r@.....

0010 7f 00 00 01 7f 00 00 01 f5 e5 00 50 6d 58 ff 15PmX..

0020 23 eb 58 72 50 18 27 f9 39 69 00 00 47 45 54 20 #.XrP.'.'9i..GET

Family (null.family), 4 bytes

Packets: 15 · Displayed: 9 (60.0%) · Dropped: 0 (0.0%) Profile: Default

سوال ۳

اعداد تنظیم شده برای فلگ های این بسته در شکل زیر نشان داده شده است.

*Adapter for loopback traffic capture

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 0

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|-----------|-------------|----------|--------|--|
| 3 | 4.396884 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 62949 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1 |
| 4 | 4.396969 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 80 → 62949 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 ... |
| 5 | 4.397034 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 62949 → 80 [ACK] Seq=1 Ack=1 Win=2619648 Len=0 |
| 9 | 4.401923 | 127.0.0.1 | 127.0.0.1 | HTTP | 595 | GET / HTTP/1.1 |

000. = Reserved: Not set
 ...0 = Nonce: Not set
0... = Congestion Window Reduced (CWR): Not set
0.. = ECN-Echo: Not set
0. = Urgent: Not set
0... = Acknowledgment: Not set
0... = Push: Not set
0.. = Reset: Not set
 >1. = Syn: Set
0 = Fin: Not set
 [TCP Flags:S.]

0000 02 00 00 00 45 00 00 34 5c 6c 40 00 80 06 00 00 ...E..4 \1@.....

Checksum Status (tcp.checksum.status) | Packets: 15 · Displayed: 9 (60.0%) · Dropped: 0 (0.0%) | Profile: Default

سوال ۴

تفاوت بسته های دو سایت، در نام هاست و پورت مقصد می باشد.

*Adapter for loopback traffic capture

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 0

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|-----------|-------------|----------|--------|--|
| 3 | 5.972994 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 62967 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1 |
| 4 | 5.973101 | 127.0.0.1 | 127.0.0.1 | TCP | 56 | 80 → 62967 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1 |
| 5 | 5.973169 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 62967 → 80 [ACK] Seq=1 Ack=1 Win=2619648 Len=0 |
| 9 | 5.981476 | 127.0.0.1 | 127.0.0.1 | HTTP | 614 | GET / HTTP/1.1 |
| 10 | 5.981525 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 80 → 62967 [ACK] Seq=1 Ack=571 Win=2619648 Len=0 |
| 11 | 5.985419 | 127.0.0.1 | 127.0.0.1 | HTTP | 248 | HTTP/1.1 304 Not Modified |
| 12 | 5.985470 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 62967 → 80 [ACK] Seq=571 Ack=205 Win=2619392 Len=0 |
| 44 | 10.998444 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 80 → 62967 [FIN, ACK] Seq=205 Ack=571 Win=2619648 Len=0 |
| 45 | 10.998500 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 62967 → 80 [ACK] Seq=571 Ack=206 Win=2619392 Len=0 |

Window: 65535
 [Calculated window size: 65535]
 Checksum: 0xce41 [unverified]
 [Checksum Status: Unverified]
 Urgent Pointer: 0
 > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted

0020 00 00 00 00 80 02 ff ff ce 41 00 00 02 04 ff d7A.....

wireshark_NPF_Loopback8DNR10.pcapng | Packets: 45 · Displayed: 9 (20.0%) | Profile: Default

سوال ۵

تصویر گواهی در زیر آورده شده است.

| Certificate | |
|--------------------------|--|
| VMware | |
| Subject Name | |
| Country | US |
| Locality | Palo Alto |
| Organizational Unit | VMware |
| Common Name | VMware |
| Email Address | none@vmware.com |
| Issuer Name | |
| Country | US |
| Locality | Palo Alto |
| Organizational Unit | VMware |
| Common Name | VMware |
| Email Address | none@vmware.com |
| Validity | |
| Not Before | Sun, 22 Mar 2020 18:07:47 GMT |
| Not After | Mon, 22 Mar 2021 18:07:47 GMT |
| Public Key Info | |
| Algorithm | RSA |
| Key Size | 2048 |
| Exponent | 65537 |
| Modulus | C6:13:A7:67:FA:12:A2:98:AC:43:54:E4:5A:FD:1E:8A:56:75:60:88:AE:5F:33:1A:88:2E... |
| Miscellaneous | |
| Serial Number | 00:DE:9D:90:48:79:4B:6B:00 |
| Signature Algorithm | SHA-256 with RSA Encryption |
| Version | 3 |
| Download | PEM (cert) PEM (chain) |
| Fingerprints | |
| SHA-256 | 6E:CD:84:E2:F6:7D:35:A6:9B:6B:45:8A:CD:41:19:8C:34:56:DB:8D:A4:9A:54:41:4D:0... |
| SHA-1 | 8B:3D:1C:8A:65:F4:3B:5F:33:3D:65:B6:2D:CA:49:98:86:C2:F0:25 |
| Basic Constraints | |
| Certificate Authority | Yes |
| Subject Key ID | |
| Key ID | 31:19:EF:5E:E3:23:5A:0C:4D:E0:7A:A1:DA:8C:A0:F1:3C:A6:8F:E4 |
| Authority Key ID | |
| Key ID | 31:19:EF:5E:E3:23:5A:0C:4D:E0:7A:A1:DA:8C:A0:F1:3C:A6:8F:E4 |

گواهی را دستگاه VMware برای خودش صادر کرده است.
اعتبار گواهی تا تاریخ ۲۲ مارس ۲۰۲۱ می باشد.
کلید عمومی از الگوریتم RSA استفاده می کند و سایز آن ۲۰۴۸ می باشد.
امضای دیجیتال از الگوریتم SHA-256 با رمزگذاری RSA انجام شده است.

سوال ۶

خیر. چون داده ها به صورت رمزگذاری شده منتقل می شوند، امکان خواندن آن ها وجود ندارد. در واقع متن پیام، بی معنی به نظر می رسند.

*Adapter for loopback traffic capture

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 1

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|-----------|-------------|----------|--------|--|
| 40 | 0.042069 | 127.0.0.1 | 127.0.0.1 | TLSv1.2 | 95 | Change Cipher Spec, Encrypted Handshake Message |
| 41 | 0.042092 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 54274 → 443 [ACK] Seq=1013 Ack=1522 Win=2618112 Len=0 |
| 42 | 0.043888 | 127.0.0.1 | 127.0.0.1 | TLSv1.2 | 387 | Application Data |
| 43 | 0.043914 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 54274 → 443 [ACK] Seq=1013 Ack=1865 Win=2617856 Len=0 |
| 48 | 0.044210 | 127.0.0.1 | 127.0.0.1 | TLSv1.2 | 75 | Encrypted Alert |
| 49 | 0.044233 | 127.0.0.1 | 127.0.0.1 | TCP | 44 | 443 → 54274 [FIN, ACK] Seq=1865 Ack=1044 Win=2619136 Len=0 |

Content Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 338
Encrypted Application Data: 7cd72deb20a7bf3345bfb1d233994181e990249a5e086a923308f3805d8174f6a100dc48...
[Application Data Protocol: http-over-tls]

| | | | | | |
|------|----|----------------------|-------------------------|---|---------------------|
| 0030 | 52 | 7c d7 2d eb 20 a7 bf | 33 45 bf b1 d2 33 99 41 | R | 3E...3.A |
| 0040 | 81 | e9 90 24 9a 5e 08 6a | 92 33 08 f3 80 5d 81 74 | | ...\$.^..j..3...].t |
| 0050 | f6 | a1 00 dc 48 9c 23 e1 | de ee 54 da cc 00 06 c7 | | ...H.#. ..T.... |
| 0060 | 37 | f5 ae ae 57 df 9f f7 | 54 0b de 43 26 8c cf 9c | | 7...W... T..C&... |
| 0070 | e3 | 21 4d 0b 97 6f cd 3c | 1d aa 1f 84 7d 71 ab fb | | .IM...o.<}q... |
| 0080 | 95 | c7 82 e3 52 97 ce 1e | ff e2 e8 24 4e 29 0a e1 | |R... ..\$N).. |
| 0090 | d5 | 32 1c e6 12 c9 6e e1 | af 2e 1e c0 1b 54 e0 5c | | -2....n... ..T\ |
| 00a0 | be | 64 5d d6 28 14 54 ab | 7d f0 d2 ed c5 07 41 df | | -d].(.T.).....A |

Payload is encrypted application data (tls.app_data), 338 bytes

Packets: 117 · Displayed: 20 (17.1%) · Dropped: 0 (0.0%) Profile: Default

سوال ۷

تصویر گواهی گوگل در زیر آورده شده است.

Certificate

| www.google.com | GTS CA 101 | GlobalSign |
|--------------------------|---|------------|
| Subject Name | | |
| Country | US | |
| State/Province | California | |
| Locality | Mountain View | |
| Organization | Google LLC | |
| Common Name | www.google.com | |
| Issuer Name | | |
| Country | US | |
| Organization | Google Trust Services | |
| Common Name | GTS CA 101 | |
| Validity | | |
| Not Before | Tue, 23 Mar 2021 08:26:20 GMT | |
| Not After | Tue, 15 Jun 2021 08:26:19 GMT | |
| Subject Alt Names | | |
| DNS Name | www.google.com | |
| Public Key Info | | |
| Algorithm | Elliptic Curve | |
| Key Size | 256 | |
| Curve | P-256 | |
| Public Value | 04:6C:92:09:1A:55:C5:09:FC:10:25:B2:80:8C:D2:90:C2:A9:C4:10:EF:75:C9:E5:AB:A9... | |
| Miscellaneous | | |
| Serial Number | 6B:5D:F1:D9:FE:8E:23:2C:03:00:00:00:00:CB:D7:61 | |
| Signature Algorithm | SHA-256 with RSA Encryption | |
| Version | 3 | |
| Download | PEM (cert) PEM (chain) | |
| Fingerprints | | |
| SHA-256 | A3:9C:CA:8B:CC:EA:61:B6:5B:2F:EB:FE:9B:A8:CC:C2:90:E2:CF:E1:DA:7F:5A:FF:4E:08:... | |
| SHA-1 | D3:C2:E2:DE:F0:94:78:07:EC:8E:EA:49:B1:1D:36:C3:67:03:60:25 | |
| Basic Constraints | | |
| Certificate Authority | No | |

| | |
|-----------------------|---|
| ● Basic Constraints | |
| Certificate Authority | No |
| ● Key Usages | |
| Purposes | Digital Signature |
| Extended Key Usages | |
| Purposes | Server Authentication |
| Subject Key ID | |
| Key ID | 85:A8:1A:44:90:5E:F4:18:BD:C7:34:3E:AD:69:F5:52:E1:F8:CE:2C |
| Authority Key ID | |
| Key ID | 98:D1:F8:6E:10:EB:CF:9B:EC:60:9F:18:90:1B:A0:E8:7D:09:FD:2B |
| CRL Endpoints | |
| Distribution Point | http://crl.plk.goog/GTS1O1core.crl |
| Authority Info (AIA) | |
| Location | http://ocsp.plk.goog/gts1o1core |
| Method | Online Certificate Status Protocol (OCSP) |
| Location | http://plk.goog/gsr2/GTS1O1.crt |
| Method | CA Issuers |
| Certificate Policies | |
| Policy | Certificate Type (2.23.140.1.2.2) |
| Value | Organization Validation |
| Policy | Statement Identifier (1.3.6.1.4.1) |
| Value | 1.3.6.1.4.1.11129.2.5.3 |
| Embedded SCTs | |
| Log ID | 7D:3E:F2:F8:8F:FF:88:55:68:24:C2:C0:CA:9E:52:89:79:2B:C5:0E:78:09:7F:2E:6A:97:6... |
| Name | Google "Xenon2021" |
| Signature Algorithm | SHA-256 ECDSA |
| Version | 1 |
| Timestamp | Tue, 23 Mar 2021 09:26:20 GMT |
| Log ID | EE:C0:95:EE:8D:72:64:0F:92:E3:C3:B9:1B:C7:12:A3:69:6A:09:7B:48:6A:1A:14:38:E6:... |
| Name | DigiCert Nettle2021 |
| Signature Algorithm | SHA-256 ECDSA |
| Version | 1 |
| Timestamp | Tue, 23 Mar 2021 09:26:20 GMT |

تفاوت های زیادی وجود دارد. از جمله تاریخ اعتبار، صادر کننده ی گواهی، کلید و نوع رمزنگاری و ...

سوال ۸

با دستور `list -l` فایل های درون دایرکتوری لیست شده اند.

*Adapter for loopback traffic capture

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|-----------|-------------|----------|--------|--|
| 197 | 0.022604 | 127.0.0.1 | 127.0.0.1 | FTP | 90 | Response: 227 Entering Passive Mode (127,0,0,1,254,25) |
| 206 | 0.023370 | 127.0.0.1 | 127.0.0.1 | FTP | 53 | Request: LIST -l |
| 212 | 0.025056 | 127.0.0.1 | 127.0.0.1 | FTP | 69 | Response: 150 Connection accepted |
| 231 | 0.025730 | 127.0.0.1 | 127.0.0.1 | FTP | 61 | Response: 226 Transfer OK |
| 233 | 0.025947 | 127.0.0.1 | 127.0.0.1 | FTP | 50 | Request: QUIT |
| 239 | 0.026670 | 127.0.0.1 | 127.0.0.1 | FTP | 57 | Response: 221 Goodbye |
| 221 | 0.025264 | 127.0.0.1 | 127.0.0.1 | FTP-DATA | 3231 | FTP Data: 3187 bytes (PASV) (LIST -l) |

> Frame 221: 3231 bytes on wire (25848 bits), 3231 bytes captured (25848 bits) on interface \Device\NPF_{...}, id 0

> Null/Loopback

> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

> Transmission Control Protocol, Src Port: 65049, Dst Port: 65050, Seq: 1, Ack: 1, Len: 3187

FTP Data (3187 bytes data)

[Setup frame: 197]

[Setup method: PASV]

[Command: LIST -l]

Command frame: 206

[Current working directory: /]

> Line-based text data (51 lines)

Frame (frame). 3.231 bytes | Packets: 277 · Displayed: 277 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

همان طور که در تصویر زیر مشخص است کاربر از یوزر `test` و رمز `123` استفاده کرده است.

پروتکل لایه ترنسپورت `TCP` می باشد.

پورت مبدا `۶۵۰۴۸` و پورت مقصد `۲۱` می باشد.

*Adapter for loopback traffic capture

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|-----------|-------------|----------|--------|--|
| 103 | 0.015848 | 127.0.0.1 | 127.0.0.1 | FTP | 55 | Request: USER test |
| 105 | 0.016777 | 127.0.0.1 | 127.0.0.1 | FTP | 76 | Response: 331 Password required for test |
| 109 | 0.016917 | 127.0.0.1 | 127.0.0.1 | FTP | 54 | Request: PASS 123 |
| 118 | 0.017584 | 127.0.0.1 | 127.0.0.1 | FTP | 59 | Response: 230 Logged on |
| 125 | 0.017814 | 127.0.0.1 | 127.0.0.1 | FTP | 50 | Request: SYST |

> Frame 103: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_{...}, id 0

> Null/Loopback

> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

> Transmission Control Protocol, Src Port: 65048, Dst Port: 21, Seq: 1, Ack: 149, Len: 11

> File Transfer Protocol (FTP)

[Current working directory:]

0000 02 00 00 00 45 00 00 33 dd ff 40 00 80 06 00 00E..3..@....

0010 7f 00 00 01 7f 00 00 01 fe 18 00 15 6d 56 73 7cmVs|

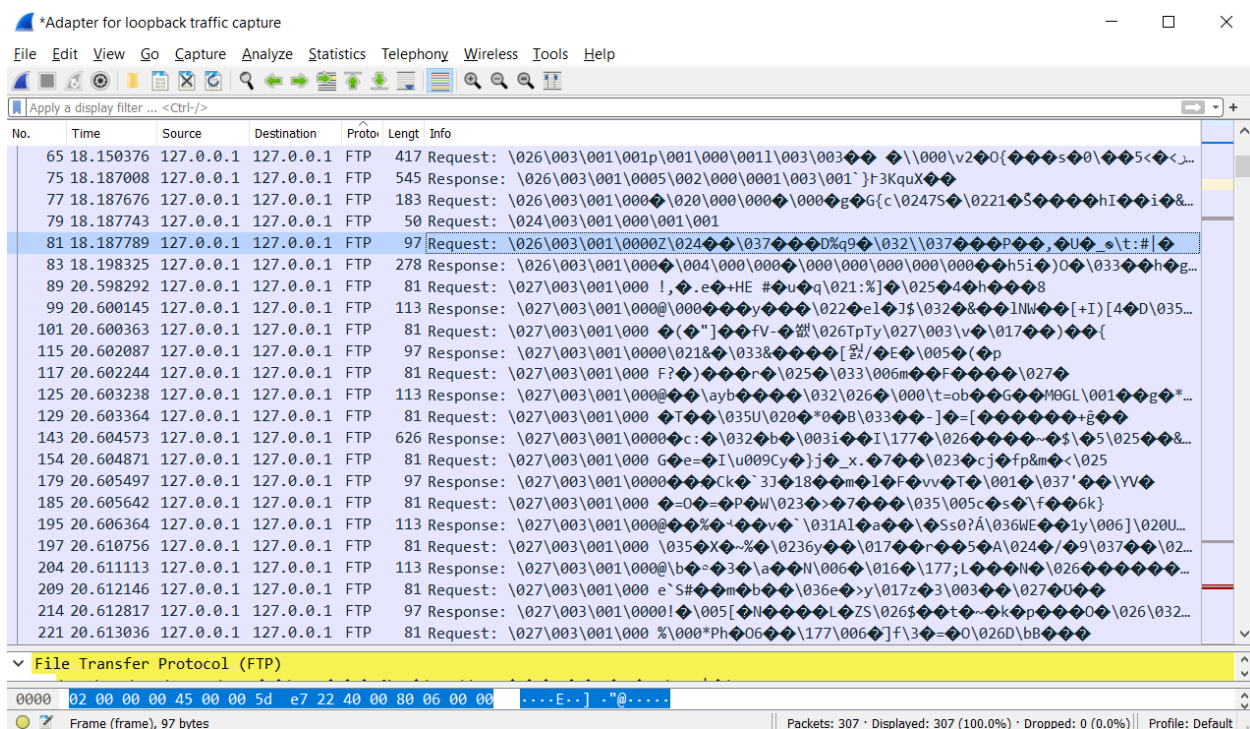
0020 82 39 19 32 50 18 27 f9 70 bf 00 00 55 53 45 52 -9-2P.p...USER

Transmission Control Protocol (tcp), 20 bytes | Packets: 277 · Displayed: 277 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

سوال ۹

بعد از فعال کردن SSL، امکان برقراری ارتباط از طریق مرورگر وجود ندارد.

با استفاده از نرم افزار FileZilla دوباره ارتباط را متصل کردیم. که چون داده ها رمزگذاری شده اند، پس قابل خواندن نیستند.



بخش پروتکل HTTP

با توجه به اینکه وبسایت اصلی دانشگاه از پروتکل https استفاده می کند. پس به سایت pbo.aut.ac.ir درخواست دادیم تا بتوان بسته های http را مشاهده کرد.

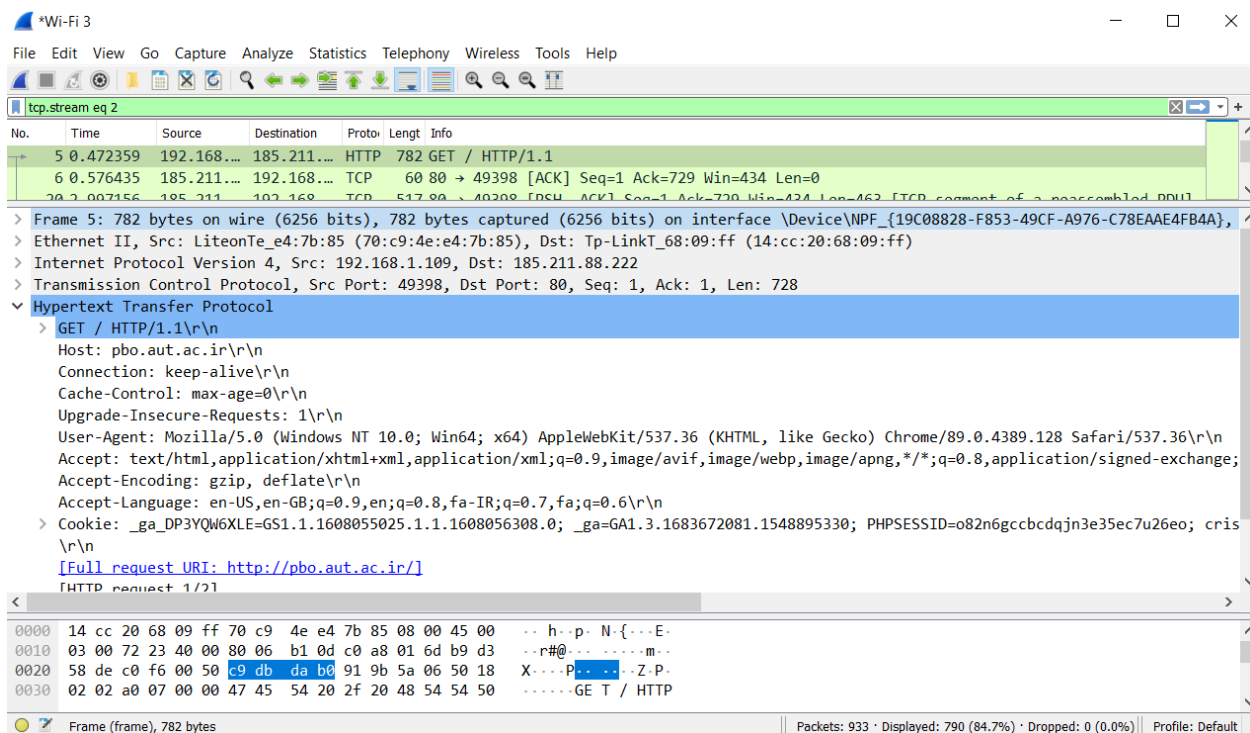
مقدار connection، keep-alive می باشد.

درخواست از نوع GET است.

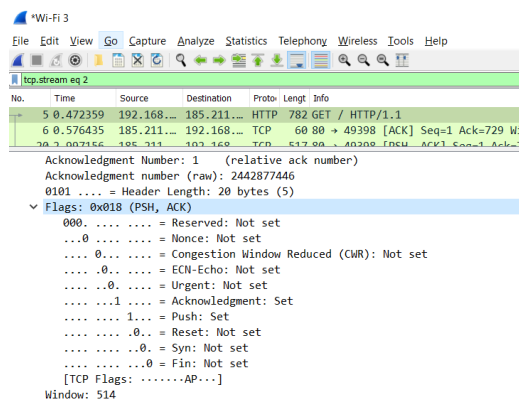
مقدار user-agent، به صورت زیر می باشد.

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.128 Safari/537.36\r\n

این مقدار بیانگر، مشخصات سیستم عامل، مرورگر و ... مربوط به کلاینت درخواست دهنده می باشد.



مقدار فلگ های مربوطه را در تصویر زیر می بینیم.



بخش پروتکل FTP

پروتکل لایه ی ترنسپورت در این بسته ها TCP می باشد.

پورت مبدا ۴۹۵۰۲ و پورت مقصد ۲۱ است.

مقدار username به صورت anonymous مشخص شده است.

مقدار password ثبت شده، chrome@example.com می باشد.

*Wi-Fi 3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 1

| No. | Time | Source | Destination | Proto | Length | Info |
|-----|----------|--------------|--------------|-------|--------|---|
| 132 | 4.453471 | 195.83.1... | 192.168.1... | FTP | 60 | Response: 220- |
| 133 | 4.494121 | 192.168.1... | 195.83.1... | TCP | 54 | 49502 → 21 [ACK] Seq=1 Ack=7 Win=131584 Len=0 |
| 135 | 4.697232 | 195.83.1... | 192.168.1... | FTP | 1038 | Response: |
| 136 | 4.697531 | 192.168.1... | 195.83.1... | FTP | 70 | Request: USER anonymous |
| 137 | 4.899661 | 195.83.1... | 192.168.1... | FTP | 103 | Response: 331 Guest login ok, type your name as password. |
| 138 | 4.899851 | 192.168.1... | 195.83.1... | FTP | 79 | Request: PASS chrome@example.com |
| 139 | 5.101404 | 195.83.1... | 192.168.1... | FTP | 60 | Response: 230- |
| 140 | 5.145263 | 192.168.1... | 195.83.1... | TCP | 54 | 49502 → 21 [ACK] Seq=42 Ack=1046 Win=130304 Len=0 |
| 141 | 5.347087 | 195.83.1... | 192.168.1... | FTP | 395 | Response: \tVous etes dans la classe guest, |
| 142 | 5.347327 | 192.168.1... | 195.83.1... | FTP | 60 | Request: SYST |

> Frame 138: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface \Device\NPF_{19C08828-F853-49CF-A976-C78EAAE4FB4A}, interface 0

> Ethernet II, Src: LiteonTe_e4:7b:85 (70:c9:4e:e4:7b:85), Dst: Tp-LinkT_68:09:ff (14:cc:20:68:09:ff)

> Internet Protocol Version 4, Src: 192.168.1.109, Dst: 195.83.118.1

> Transmission Control Protocol, Src Port: 49502, Dst Port: 21, Seq: 17, Ack: 1040, Len: 25

> File Transfer Protocol (FTP)

[Current working directory:]

0010 00 41 30 78 40 00 80 06 ce d4 c0 a8 01 6d c3 53 -A0x@... ..m.S

0020 76 01 c1 5e 00 15 6d 34 89 77 fe 83 bd 45 50 18 v...^...m4 -w...EP-

0030 01 fe c6 4c 00 00 50 41 53 53 20 63 68 72 6f 6d ---L...PA SS chrom

Transmission Control Protocol (tcp), 20 bytes

Packets: 222 · Displayed: 33 (14.9%) · Dropped: 0 (0.0%) Profile: Default