

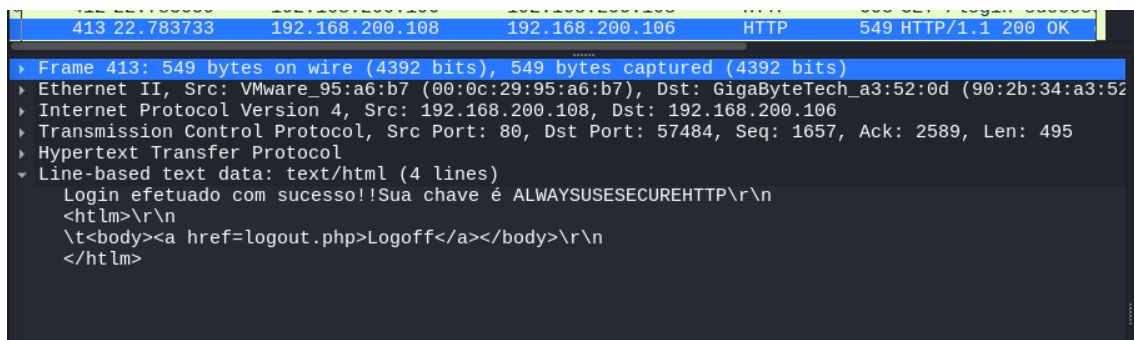
## LABORATÓRIO E ATIVIDADE - ANALISANDO SERVICOS HTTP E HTTPS (WIRESHARK):

Nome: Enzo Arrue

1. **Inseguro:** Existe um trafego inseguro nesta captura.  
Analisando o arquivo inseguro.dump

1.1. Descubra a chave e submeta juntamente com o nome do protocolo inseguro que está sendo utilizado.

Formato da resposta : PROTOCOLO:CHAVE



HTTP: ALWAYSUSESECUREHTTP

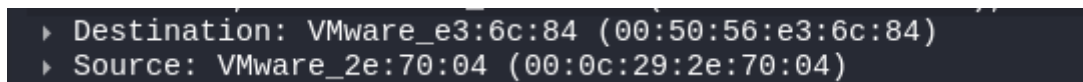
1.2. Identifique a versão do servidor inseguro que está sendo utilizado.

OPENSSH6.1 HTTP/1.1

2. **Texto Puro:** O uso de conexões não criptografadas coloca seus dados em risco. As pessoas podem roubar suas informações capturando os dados que você envia por uma rede não segura, como o wi-fi em uma cafeteria. O atacante descobriu a senha quando se conectou a um fórum de suporte técnico.

Analisando o arquivo textopuro.pcap responda:

2.1. Quais endereços físicos (atacante e do alvo)?



2.2. Quais endereços IPs (atacante e alvo)?

Source: 172.16.86.130

Destination: 108.168.252.20

2.3. Quais as portas usadas (atacante e alvo)?

Source port: 50004

Destination port: 80

2.4. Qual o servidor usado na máquina alvo?

```
HTTP/1.1 200 OK
Date: Wed, 07 Jun 2017 03:50:43 GMT
Server: Apache
X-Powered-By: PHP/5.4.45-0+deb7u8
Set-Cookie: bblastactivity=0; expires=
Cache-Control: private
Pragma: private
X-UA-Compatible: IE=7
```

2.5. Durante a troca de mensagens, qual foi o usuário e senha encontrado?

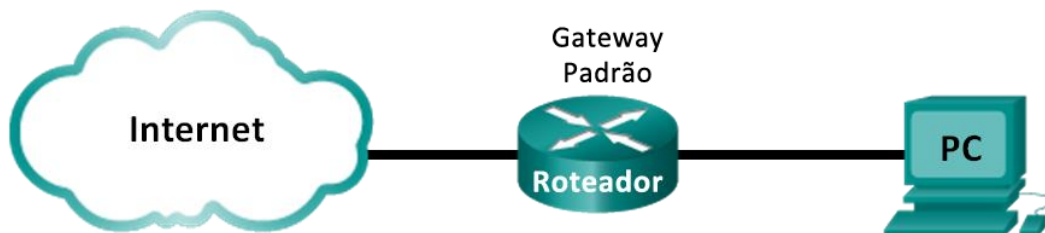
Formato da resposta : usuário , senha

NotOrc, Checkers86

```
▶ Form item: "vb_login_username" = "NotOrc"
▶ Form item: "vb_login_password" = "Checkers86!"
▶ Form item: "s" = ""
▶ Form item: "securitytoken" = "guest"
▶ Form item: "do" = "login"
▶ Form item: "vb_login_md5password" = ""
▶ Form item: "vb_login_md5password_utf" = ""
```

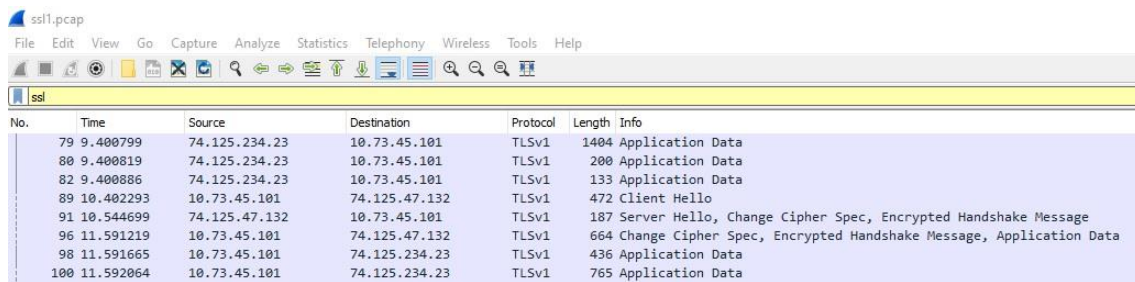
3. Cenário **https** com acesso ao servidor **https** (Cenário 1). Considere o seguinte procedimento:

**Topologia – Cenário 1:**



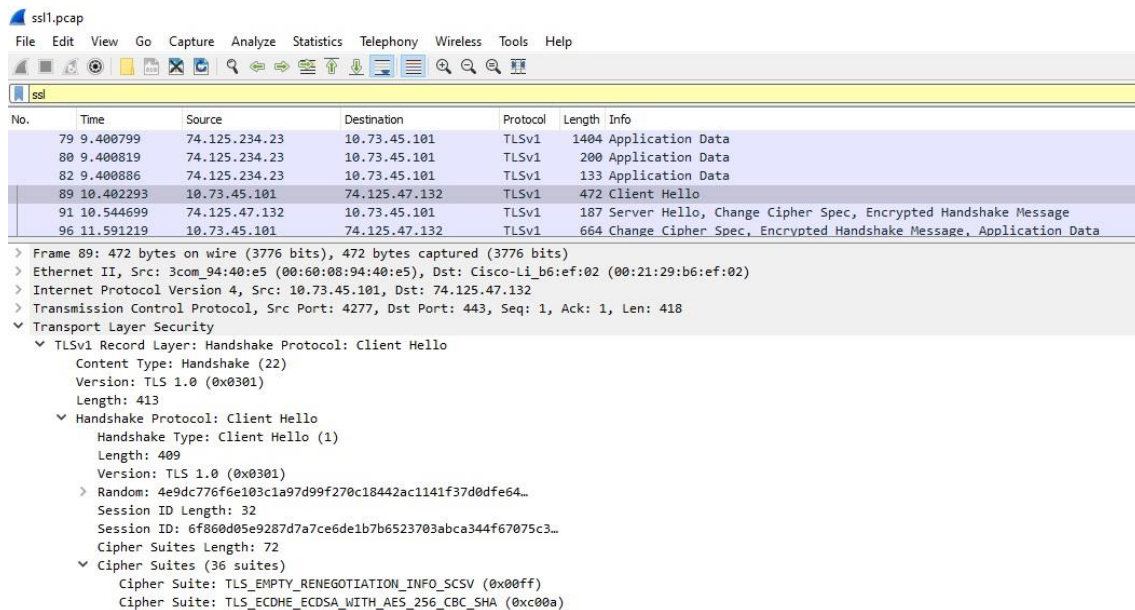
a. Iniciar a captura com o Wireshark → acessar uma página https (Office 365 ou outro site https) → iniciar a conexão da página, capturar pacotes e na sequência finalizar a conexão e captura com o Wireshark.

b. Após a captura no Wireshark, filtre o tráfego https com **SSL** ou **TLS**.



No.	Time	Source	Destination	Protocol	Length	Info
79	9.400799	74.125.234.23	10.73.45.101	TLSv1	1404	Application Data
80	9.400819	74.125.234.23	10.73.45.101	TLSv1	200	Application Data
82	9.400886	74.125.234.23	10.73.45.101	TLSv1	133	Application Data
89	10.402293	10.73.45.101	74.125.47.132	TLSv1	472	Client Hello
91	10.544699	74.125.47.132	10.73.45.101	TLSv1	187	Server Hello, Change Cipher Spec, Encrypted Handshake Message
96	11.591219	10.73.45.101	74.125.47.132	TLSv1	664	Change Cipher Spec, Encrypted Handshake Message, Application Data
98	11.591665	10.73.45.101	74.125.234.23	TLSv1	436	Application Data
100	11.592064	10.73.45.101	74.125.234.23	TLSv1	765	Application Data

c. Identifique o conjunto de cifras com as sinalizações **Client Hello** e **Server Hello**.



No.	Time	Source	Destination	Protocol	Length	Info
79	9.400799	74.125.234.23	10.73.45.101	TLSv1	1404	Application Data
80	9.400819	74.125.234.23	10.73.45.101	TLSv1	200	Application Data
82	9.400886	74.125.234.23	10.73.45.101	TLSv1	133	Application Data
89	10.402293	10.73.45.101	74.125.47.132	TLSv1	472	Client Hello
91	10.544699	74.125.47.132	10.73.45.101	TLSv1	187	Server Hello, Change Cipher Spec, Encrypted Handshake Message
96	11.591219	10.73.45.101	74.125.47.132	TLSv1	664	Change Cipher Spec, Encrypted Handshake Message, Application Data

> Frame 89: 472 bytes on wire (3776 bits), 472 bytes captured (3776 bits)

> Ethernet II, Src: 3com\_94:40:e5 (00:60:08:94:40:e5), Dst: Cisco-Li\_b6:ef:02 (00:21:29:b6:ef:02)

> Internet Protocol Version 4, Src: 10.73.45.101, Dst: 74.125.47.132

> Transmission Control Protocol, Src Port: 4277, Dst Port: 443, Seq: 1, Ack: 1, Len: 418

▼ Transport Layer Security

▼ TLSv1 Record Layer: Handshake Protocol: Client Hello

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 413

▼ Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 409

Version: TLS 1.0 (0x0301)

> Random: 4e9dc776f6e103c1a97d99f270c18442ac1141f37d0dfe64...

Session ID Length: 32

Session ID: 6f860d05e9287d7a7ce6de1b7b6523703abca344f67075c3...

Cipher Suites Length: 72

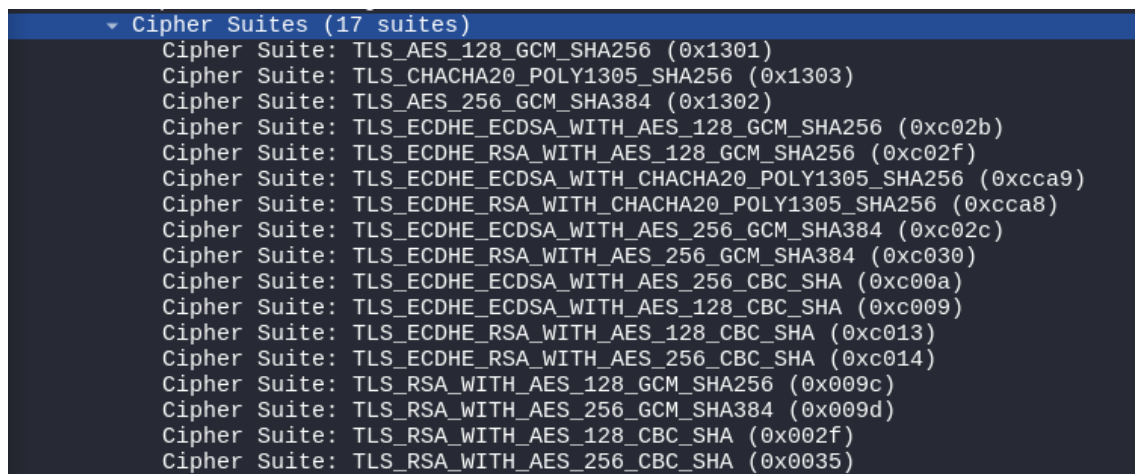
▼ Cipher Suites (36 suites)

Cipher Suite: TLS\_EMPTY\_RENEGOTIATION\_INFO\_SCSV (0x00ff)

Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA (0xc00a)

c.1. A partir de uma captura de dados (Wireshark) usando SSL/TLS, pede-se:

a. Identificar 3 séries de cifras usadas na sinalização “**client hello**”. Explique o que ocorre no estabelecimento de conexão com o servidor.



Cipher Suite	Hex Value
TLS_AES_128_GCM_SHA256	0x1301
TLS_CHACHA20_POLY1305_SHA256	0x1303
TLS_AES_256_GCM_SHA384	0x1302
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	0xc02b
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0xc02f
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	0xc030
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	0xc031
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	0xc032
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	0xc033
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	0xc00a
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	0xc009
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	0xc013
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	0xc014
TLS_RSA_WITH_AES_128_GCM_SHA256	0x009c
TLS_RSA_WITH_AES_256_GCM_SHA384	0x009d
TLS_RSA_WITH_AES_128_CBC_SHA	0x002f
TLS_RSA_WITH_AES_256_CBC_SHA	0x0035

O cliente propõe várias cifras, e o servidor escolherá uma para usar.

c.2. Qual a série de cifra usada na sinalização “**server hello**” considerando algoritmo de chave simétrica, assimétrica e hash envolvidos para essa sinalização? Explique o conjunto de cifras.

6590	6.493985917	2020:1ec:0d1::33	2804:14d:7893:87e0:...	TLSv1.3	2842 Server Hello, Change Ciph
6653	6.725087007	2620:1ec:bdf::33	2804:14d:7893:87e0:...	TLSv1.3	2842 Server Hello, Change Ciph
6783	8.360857221	20.189.173.8	192.168.0.192	TLSv1.3	2962 Server Hello, Change Ciph
6789	8.380069767	20.189.173.8	192.168.0.192	TLSv1.3	6446 Server Hello, Change Ciph

```

Transport Layer Security
  TLSv1.3 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 155
  Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 151
  Version: TLS 1.2 (0x0303)
    [Expert Info (Chat/Deprecated): This legacy_version field MUST be ignored. The supported_versions extension is used for this purpose.]
    Random: 64221bceeb7d8b4cd263ff9c8e117f44c0b215b72b99d5d2ba6100fc8f3d6c2b
    Session ID Length: 32
    Session ID: 3aea0ffb33d549f647ce8455724b5c21f0c38471c657e3c973dee43dfdb7150b
    Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
    Compression Method: null (0)
    Extensions Length: 79
    Extension: supported_versions (len=2) TLS 1.3
    Extension: key_share (len=69) secp256r1
      [JA3S Fullstring: 771,4866,43-51]
      [JA3S: 15af977ce25de452b96affa2adddb1036]
  TLSv1.3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
    Content Type: Change Cipher Spec (20)
  
```

TLS\_AES\_256\_GCM\_SHA384 > AES 256 criptografia Sim > GCM criptografia e autenticação > SHA384 handshake e HMAC

c.3. Quais IPs (cliente e servidor) e as portas associadas (cliente e servidor). Qual a versão do protocolo TLS?

6650	6.710230254	2804:14d:7893:87e0:...	2620:1ec:bdf::33	TLSv1.3	744 Client Hello (SNI=
6778	8.173027677	192.168.0.192	20.189.173.8	TLSv1.3	747 Client Hello (SNI=
6781	8.183041608	192.168.0.192	20.189.173.8	TLSv1.3	747 Client Hello (SNI=

```

> Frame 6778: 747 bytes on wire (5976 bits), 747 bytes captured (5976 bits) on interface eth0, id
> Ethernet II, Src: PCSSystemtec_04:42:0f (08:00:27:04:42:0f), Dst: 06:02:b8:62:42:d6 (06:02:b8:6
> Internet Protocol Version 4, Src: 192.168.0.192, Dst: 20.189.173.8
> Transmission Control Protocol, Src Port: 55776, Dst Port: 443, Seq: 1, Ack: 1, Len: 681
> Transport Layer Security

```

Src 192.168.0.192 cliente

Dst 20.189.173.8 servidor

Src port 55776

Dst port: 443 web https

TLS 1.2

c.4. Com relação ao certificado SSL/TLS encontrado, responda. Qual a versão, os algoritmos usados, nome da organização, país, validade do certificado.

```

Certificate [...]: 308205ac30820494a00302010202100efb7e547edf0ff1069aee57696d7ba0300d06092a864886f70d
  signedCertificate
    version: v3 (2)
    serialNumber: 0x0efb7e547edf0ff1069aee57696d7ba0
    signature (sha384WithRSAEncryption)
      Algorithm Id: 1.2.840.113549.1.1.12 (sha384WithRSAEncryption)
    issuer: rdnSequence (0)
    rdnSequence: 4 items (id-at-commonName=DigiCert Global Root G2,id-at-organizationalUnitName=
      RDNSquence item: 1 item (id-at-countryName=US)
      RDNSquence item: 1 item (id-at-organizationName=DigiCert Inc)
      RDNSquence item: 1 item (id-at-organizationalUnitName=www.digicert.com)
      RDNSquence item: 1 item (id-at-commonName=DigiCert Global Root G2)
    validity
      notBefore: utcTime (0)
        utcTime: 2023-06-08 00:00:00 (UTC)
      notAfter: utcTime (0)
        utcTime: 2026-08-25 23:59:59 (UTC)

```

Alg: SHA384 com Encriptação RSA

País: US > Estados Unidos

Organização: DigiCert Inc

Validade: Não antes de 08 do 06 de 2023 e não depois de 25 do 08 de 2026.