

Matei Vlad Cristian  
321 CC

Laborator

1.

Algoritmul folosit pentru semnarea certificatului :

sha256WithRSAEncryption

Entitatea care a eliberat certificatul :

Issuer: C = US, O = Google Trust Services, CN = GTS CA 1O1

Intervalul de timp in care certificatul e valid :

Validity

Not Before: May 3 09:02:30 2021 GMT

Not After : Jul 26 09:02:29 2021 GMT

Cheia publica :

Subject Public Key Info:

Public Key Algorithm: id-ecPublicKey

Public-Key: (256 bit)

pub:

04:f7:f7:de:4d:af:d6:b4:ca:b5:49:1f:df:90:71:  
cd:f6:cb:b7:fd:7a:d9:db:39:e4:93:68:2c:9d:55:  
fb:1f:30:4e:75:e0:ef:58:29:4c:ac:66:3e:02:63:  
f5:e2:3f:bc:2c:e1:55:3d:ae:d8:54:95:84:03:7c:  
3f:7b:d5:2f:25

ASN1 OID: prime256v1

NIST CURVE: P-256

2.

Activities Applications Wireshark Sun May 30 2013

\*wlo1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
813	3.175531394	192.168.1.101	34.118.48.238	HTTP	418	GET /favicon.ico HTTP/1.1
824	3.219463528	34.118.48.238	192.168.1.101	HTTP	688	HTTP/1.1 404 Not Found (text/html)
6716	22.671250751	192.168.1.101	34.118.48.238	HTTP	502	GET /api/v1/dummy?asasa=sasa2 HTTP/1.1
6818	22.118106669	34.118.48.238	192.168.1.101	HTTP	468	HTTP/1.1 304 Not Modified
7119	22.748670799	192.168.1.101	34.118.48.238	HTTP	502	GET /api/v1/dummy?asasa=sasa2 HTTP/1.1
7169	22.794699191	34.118.48.238	192.168.1.101	HTTP	468	HTTP/1.1 304 Not Modified
7319	23.158992616	192.168.1.101	34.118.48.238	HTTP	502	GET /api/v1/dummy?asasa=sasa2 HTTP/1.1
7363	23.197304269	34.118.48.238	192.168.1.101	HTTP	468	HTTP/1.1 304 Not Modified
7482	23.436902884	192.168.1.101	34.118.48.238	HTTP	502	GET /api/v1/dummy?asasa=sasa2 HTTP/1.1
7512	23.483155706	34.118.48.238	192.168.1.101	HTTP	468	HTTP/1.1 304 Not Modified
7593	23.761270094	192.168.1.101	34.118.48.238	HTTP	502	GET /api/v1/dummy?asasa=sasa2 HTTP/1.1
7630	23.740728032	34.118.48.238	192.168.1.101	HTTP	468	HTTP/1.1 304 Not Modified
21206	51.369740337	192.168.1.101	103.7.8.233	HTTP	393	GET / HTTP/1.1
21523	51.927186688	103.7.8.233	192.168.1.101	HTTP	71	HTTP/1.1 301 Moved Permanently (text/html) (text/html)
32437	77.938929688	192.168.1.101	216.58.214.195	OCSP	451	Request
32471	77.999495313	216.58.214.195	192.168.1.101	OCSP	767	Response
32570	78.116407369	192.168.1.101	216.58.214.195	OCSP	451	Request
32599	78.180766587	216.58.214.195	192.168.1.101	OCSP	767	Response
33267	79.221895545	192.168.1.101	18.192.172.30	HTTP	447	GET /login.php HTTP/1.1
33297	79.259419763	18.192.172.30	192.168.1.101	HTTP	2814	HTTP/1.1 200 OK (text/html)
33309	79.296635950	192.168.1.101	18.192.172.30	HTTP	374	GET /style.css HTTP/1.1
33336	79.326549587	18.192.172.30	192.168.1.101	HTTP	2692	HTTP/1.1 200 OK (text/css)
33344	79.334439140	192.168.1.101	18.192.172.30	HTTP	376	GET /images/logo.gif HTTP/1.1
33363	79.375289134	18.192.172.30	192.168.1.101	HTTP	1014	HTTP/1.1 200 OK (GIF89a)
33366	79.376243668	192.168.1.101	18.192.172.30	HTTP	372	GET /favicon.ico HTTP/1.1
33382	79.417924911	18.192.172.30	192.168.1.101	HTTP	960	HTTP/1.1 200 OK (image/x-icon)
35240	83.105683729	192.168.1.101	18.192.172.30	HTTP	593	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
35286	83.140963276	18.192.172.30	192.168.1.101	HTTP	342	HTTP/1.1 302 Found (text/html)
35288	83.140897932	192.168.1.101	18.192.172.30	HTTP	460	GET /login.php HTTP/1.1
35295	83.180810314	18.192.172.30	192.168.1.101	HTTP	2814	HTTP/1.1 200 OK (text/html)

[Expert Info (Chat/Sequence): GET /login.php HTTP/1.1/vr\n]  
Request Method: GET  
Request URI: /login.php  
Request Version: HTTP/1.1  
Host: testphp.vulnweb.com/vr\nUser-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:88.0) Gecko/20100101 Firefox/88.0/vr\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8/vr\nAccept-Encoding: gzip, deflate/vr\nReferer: https://www.google.com/vr\nConnection: keep-alive/vr\nUpgrade-Insecure-Requests: 1/vr\nvr\n[Full request URI: http://testphp.vulnweb.com/login.php]  
[HTTP request 1/2]  
Response in frame: 33297  
Next request in frame: 33309

0000 08 de d0 f9 82 56 c5 05 e5 76 65 88 06 45 00 .....P...ve E  
0010 01 b1 b0 2f 40 00 40 06 08 2c c9 a8 81 65 12 c0 .../0...e-  
0020 ac 1e c3 be 00 50 2e 34 26 1c 9b a7 af 68 80 18 .....P 4 & c- h-  
0030 01 f6 a8 81 00 00 01 01 08 0a 13 63 f9 91 e9 06 00 .....c 7-  
0040 50 11 47 45 54 29 2f 6c 6f 67 69 6e 2e 70 68 70 P.GET /login.php  
0050 20 40 54 50 2f 31 31 38 2e 34 38 2e 32 33 38 3a 38 39 38 4.118.48.238:8080  
0060 20 74 65 73 74 70 68 70 2e 76 75 0c 6e 77 65 62 testphp.vulnweb  
0070 26 63 0f 6d 00 6a 55 73 65 72 2d 41 67 65 6e 74 .com-Us er-Agent:  
0080 3a 28 4d 6f 7a 69 6c 6c 6f 2f 35 2e 38 29 28 58 Mozilla/5.0 (X11;  
0090 31 31 3b 2b 55 62 75 6e 74 75 2b 2d 4c 69 66 75 ; Ubuntu; Linu

wireshark\_wlo1\_2021053021022\_6Hf3TC.pcapng Packets: 39416 · Displayed: 32 (0.1%) · Dropped: 0 (0.0%) Profile: Default

Activities Applications Wireshark Sun May 30 2014

\*wlo1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
813	3.175531394	192.168.1.101	34.118.48.238	HTTP	418	GET /favicon.ico HTTP/1.1
824	3.219463528	34.118.48.238	192.168.1.101	HTTP	688	HTTP/1.1 404 Not Found (text/html)
6716	22.671250751	192.168.1.101	34.118.48.238	HTTP	502	GET /api/v1/dummy?asasa=sasa2 HTTP/1.1
6818	22.118106669	34.118.48.238	192.168.1.101	HTTP	468	HTTP/1.1 304 Not Modified
7119	22.748670799	192.168.1.101	34.118.48.238	HTTP	502	GET /api/v1/dummy?asasa=sasa2 HTTP/1.1
7169	22.794699191	34.118.48.238	192.168.1.101	HTTP	468	HTTP/1.1 304 Not Modified
7319	23.158992616	192.168.1.101	34.118.48.238	HTTP	502	GET /api/v1/dummy?asasa=sasa2 HTTP/1.1
7363	23.197304269	34.118.48.238	192.168.1.101	HTTP	468	HTTP/1.1 304 Not Modified
7482	23.436902884	192.168.1.101	34.118.48.238	HTTP	502	GET /api/v1/dummy?asasa=sasa2 HTTP/1.1
7512	23.483155706	34.118.48.238	192.168.1.101	HTTP	468	HTTP/1.1 304 Not Modified
21206	51.369740337	192.168.1.101	103.7.8.233	HTTP	393	GET / HTTP/1.1
21523	51.927186688	103.7.8.233	192.168.1.101	HTTP	71	HTTP/1.1 301 Moved Permanently (text/html) (text/html)
32437	77.938929688	192.168.1.101	216.58.214.195	OCSP	451	Request
32471	77.999495313	216.58.214.195	192.168.1.101	OCSP	767	Response
32570	78.116407369	192.168.1.101	216.58.214.195	OCSP	451	Request
32599	78.180766587	216.58.214.195	192.168.1.101	OCSP	767	Response
33267	79.221895545	192.168.1.101	18.192.172.30	HTTP	447	GET /login.php HTTP/1.1
33297	79.259419763	18.192.172.30	192.168.1.101	HTTP	2814	HTTP/1.1 200 OK (text/html)
33309	79.296635950	192.168.1.101	18.192.172.30	HTTP	374	GET /style.css HTTP/1.1
33336	79.326549587	18.192.172.30	192.168.1.101	HTTP	2692	HTTP/1.1 200 OK (text/css)
33344	79.334439140	192.168.1.101	18.192.172.30	HTTP	376	GET /images/logo.gif HTTP/1.1
33363	79.375289134	18.192.172.30	192.168.1.101	HTTP	1014	HTTP/1.1 200 OK (GIF89a)
33366	79.376243668	192.168.1.101	18.192.172.30	HTTP	372	GET /favicon.ico HTTP/1.1
33382	79.417924911	18.192.172.30	192.168.1.101	HTTP	960	HTTP/1.1 200 OK (image/x-icon)
35240	83.105683729	192.168.1.101	18.192.172.30	HTTP	593	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
35286	83.140963276	18.192.172.30	192.168.1.101	HTTP	342	HTTP/1.1 302 Found (text/html)
35288	83.140897932	192.168.1.101	18.192.172.30	HTTP	460	GET /login.php HTTP/1.1
35295	83.180810314	18.192.172.30	192.168.1.101	HTTP	2814	HTTP/1.1 200 OK (text/html)

[Expert Info (Chat/Sequence): GET /api/v1/dummy?asasa=sasa2 HTTP/1.1/vr\n]  
Request Method: GET  
Request URI: /api/v1/dummy?asasa=sasa2  
Request Version: HTTP/1.1  
Host: 34.118.48.238:8080/api/v1/dummy?asasa=sasa2  
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:88.0) Gecko/20100101 Firefox/88.0/vr\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8/vr\nAccept-Encoding: gzip, deflate/vr\nConnection: keep-alive/vr\nUpgrade-Insecure-Requests: 1/vr\nIf-None-Match: W/"c-aanL5C22098NLTyiv4pW0hniQ"/vr\nCache-Control: max-age=0/vr\nvr\n[Full request URI: http://34.118.48.238:8080/api/v1/dummy?asasa=sasa2]  
[HTTP request 5/5]

0000 08 de d0 f9 82 56 c5 05 e5 76 65 88 06 45 00 .....P...ve E  
0010 01 b1 b0 2f 40 00 40 06 08 2c c9 a8 81 65 12 c0 .../0...e-  
0020 ac 1e c3 be 00 50 2e 34 26 1c 9b a7 af 68 80 18 .....P 4 & c- h-  
0030 01 f6 a8 81 00 00 01 01 08 0a 13 63 f9 91 e9 06 00 .....c 7-  
0040 50 11 47 45 54 29 2f 6c 6f 67 69 6e 2e 70 68 70 P.GET /api/v1/dum  
0050 60 6d 70 3f 73 61 73 61 34 73 61 73 61 32 20 40 my?asasa=sasa2 H  
0060 54 54 50 2f 31 31 38 2e 34 38 2e 32 33 38 3a 38 39 38 TTP/1.1 Host: 3  
0070 34 2e 31 31 3b 2b 55 62 75 6e 74 75 2b 2d 4c 69 66 75 4.118.48.238:8080  
0080 30 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 40 0-User-Agent: M  
0090 67 7a 69 6c 6c 6f 2f 35 2e 38 29 28 58 Mozilla/5.0 (X11;

wireshark\_wlo1\_2021053021022\_6Hf3TC.pcapng Packets: 39416 · Displayed: 32 (0.1%) · Dropped: 0 (0.0%) Profile: Default

Wireshark interface showing a packet capture on the \*wlo1 interface. The packet list displays various HTTP requests and responses, including GET requests for /favicon.ico, /style.css, /images/logo.gif, and /login.php. The packet details pane shows the structure of the selected HTTP request (GET /login.php), including the request line, headers (Host, User-Agent, Accept, Accept-Language, Accept-Encoding, Referer, Connection, Upgrade-Insecure-Requests), and the request body (Vrtn).

3.

Wireshark interface showing a packet capture on the \*wlo1 interface. The packet list displays various TLSv1.2 records, including the Client Hello, Server Hello, Change Cipher Spec, and Encrypted Handshake Message. The packet details pane shows the structure of the selected TLSv1.2 record (Client Hello), including the handshake protocol, content type, and the handshake message structure (Handshake Protocol, Change Cipher Spec, Encrypted Handshake Message).

Activities Applications Wireshark Sun May 30 20:30

\*wlo1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

11s

No.	Time	Source	Destination	Protocol	Length	Info
1364	3.614006680	192.168.1.101	162.159.138.234	TLSv1.2	139	Application Data
1372	3.622998466	192.168.1.101	162.159.138.234	TLSv1.2	139	Application Data
1640	3.925181415	192.168.1.101	162.159.138.234	TLSv1.2	139	Application Data
1684	4.004186657	192.168.1.101	162.159.138.234	TLSv1.2	139	Application Data
2026	4.593422612	192.168.1.101	162.159.138.234	TLSv1.2	139	Application Data
2030	4.602219143	192.168.1.101	162.159.138.234	TLSv1.2	139	Application Data
2476	5.354927613	192.168.1.101	162.159.138.234	TLSv1.2	139	Application Data
2534	5.482908817	192.168.1.101	162.159.138.234	TLSv1.2	139	Application Data
2551	5.508093335	192.168.1.101	23.111.8.154	TLSv1.2	611	Client Hello
2553	5.503363929	192.168.1.101	23.111.8.154	TLSv1.2	611	Client Hello
2570	5.542535172	23.111.8.154	192.168.1.101	TLSv1.2	210	Server Hello, Change Cipher Spec, Encrypted Handshake Message
2572	5.542554471	23.111.8.154	192.168.1.101	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
2579	5.548208237	23.111.8.154	192.168.1.101	TLSv1.2	210	Server Hello, Change Cipher Spec, Encrypted Handshake Message
2581	5.548492890	192.168.1.101	23.111.8.154	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
2675	5.789885477	192.168.1.101	162.159.138.234	TLSv1.2	139	Application Data
2685	5.808192167	192.168.1.101	162.159.138.234	TLSv1.2	139	Application Data
2823	6.114939323	192.168.1.101	162.159.138.234	TLSv1.2	139	Application Data
2829	6.123844456	192.168.1.101	162.159.138.234	TLSv1.2	139	Application Data
3004	6.448849934	192.168.1.101	162.159.138.234	TLSv1.2	139	Application Data

Version: 1.2 (0x0303)

Random: 77350f7283e53c75d7c532175cab76b4590d328707c33886.

Session ID Length: 32

Session ID: 13fcb4eb4b5badff3d2ad0c5448163ad4b975b0bbca77d.

Cipher Suites Length: 36

- Cipher Suite: TLS\_AES\_128\_GCM\_SHA256 (0x1301)
- Cipher Suite: TLS\_CHACHA20\_POLY1305\_SHA256 (0x1303)
- Cipher Suite: TLS\_AES\_256\_GCM\_SHA384 (0x1302)
- Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02b)
- Cipher Suite: TLS\_ECDHE\_ECDSA\_WITH\_CHACHA20\_POLY1305\_SHA256 (0xc0a9)
- Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256 (0xc0ac)
- 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\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0x009c)
- Cipher Suite: TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0x009d)
- Cipher Suite: TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA (0x000f)
- Cipher Suite: TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x0035)
- Cipher Suite: TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (0x000a)

Compression Methods Length: 1

Compression Methods (1 method)

Extensions Length: 439

- Extension: server\_name (len=19)

0000 08 00 f0 32 50 dc f5 05 e5 76 65 00 00 45 00 ... p ... ve E

0010 02 55 8c 5f 40 00 00 06 ca 20 c9 a8 01 65 17 0f ... U ... e o

0020 00 9a e1 04 01 00 a2 f7 96 65 42 64 70 5b 10 ... B ... o

0030 01 fe cd 71 00 00 16 03 01 02 28 01 00 02 24 03 ... q ... ( ... s

0040 03 77 35 07 32 83 e5 3c 75 07 c5 32 17 5c a0 76 ... u ... u 2 \ v

0050 04 50 0d 32 87 07 c3 38 00 c8 f0 02 03 c2 f0 ... Y 2 - 8 - p

0060 00 20 13 fc be 4d b4 5b ad ff 3d 23 ad dc 54 40 ... M [ ... s - TH

0070 15 3a 04 b9 97 5b 0b bc a7 70 32 f4 97 05 04 ... [ ... ] 28 7

0080 0f 45 00 24 13 01 13 03 12 02 c9 2b c9 2f cc a9 ... E S ... / -

0090 cc a8 c0 2c c0 38 c0 0a c0 09 c0 13 c0 14 00 9c ... 0 ...

Transport Layer Security: Protocol Packets: 5244 · Displayed: 52 (1.0%) · Dropped: 0 (0.0%) Profile: Default

## Cea aleasa de server:

Activities Applications Wireshark Sun May 30 20:31

\*wlo1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

11s

No.	Time	Source	Destination	Protocol	Length	Info
1364	3.614006680	192.168.1.101	162.159.138.234	TLSv1.2	139	Application Data
1372	3.622998466	192.168.1.101	162.159.138.234	TLSv1.2	139	Application Data
1640	3.925181415	192.168.1.101	162.159.138.234	TLSv1.2	139	Application Data
1684	4.004186657	192.168.1.101	162.159.138.234	TLSv1.2	139	Application Data
2026	4.593422612	192.168.1.101	162.159.138.234	TLSv1.2	139	Application Data
2030	4.602219143	192.168.1.101	162.159.138.234	TLSv1.2	139	Application Data
2476	5.354927613	192.168.1.101	162.159.138.234	TLSv1.2	139	Application Data
2534	5.482908817	192.168.1.101	162.159.138.234	TLSv1.2	139	Application Data
2551	5.508093335	192.168.1.101	23.111.8.154	TLSv1.2	611	Client Hello
2553	5.503363929	192.168.1.101	23.111.8.154	TLSv1.2	611	Client Hello
2570	5.542535172	192.168.1.101	23.111.8.154	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
2572	5.542554471	23.111.8.154	192.168.1.101	TLSv1.2	210	Server Hello, Change Cipher Spec, Encrypted Handshake Message
2579	5.548208237	23.111.8.154	192.168.1.101	TLSv1.2	210	Server Hello, Change Cipher Spec, Encrypted Handshake Message
2581	5.548492890	192.168.1.101	23.111.8.154	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
2675	5.789885477	192.168.1.101	162.159.138.234	TLSv1.2	139	Application Data
2685	5.808192167	192.168.1.101	162.159.138.234	TLSv1.2	139	Application Data
2823	6.114939323	192.168.1.101	162.159.138.234	TLSv1.2	139	Application Data
2829	6.123844456	192.168.1.101	162.159.138.234	TLSv1.2	139	Application Data
3004	6.448849934	192.168.1.101	162.159.138.234	TLSv1.2	139	Application Data

[Checksum Status: Unverified]

Urgent pointer: 0

- [SEQ/ACK analysis]
- [Timestamps]

Transport Layer Security

- TLSv1.2 Record Layer: Handshake Protocol: Server Hello
- Content Type: Handshake (22)
- Version: TLS 1.2 (0x0303)
- Length: 100
- Handshake Protocol: Server Hello
- Handshake Type: Server Hello (2)
- Length: 96
- Version: TLS 1.2 (0x0303)
- Random: f5e31da9f5da5601a8e729f0b37506493177d78c2765ea.
- Session ID Length: 32
- Session ID: 13fcb4eb4b5badff3d2ad0c5448163ad4b975b0bbca77d.
- Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02f)
- Compression Method: null (0)
- Extensions Length: 24
- Extension: renegotiation\_info (len=1)
- Extension: status\_request (len=0)
- Extension: application\_layer\_protocol\_negotiation (len=11)
- TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
- Content Type: Change Cipher Spec (20)
- Version: TLS 1.2 (0x0303)
- Length: 1
- Change Cipher Spec Message
- Expert Info (Note/Sequence): This session reuses previously negotiated keys (Session resumption)!

0040 08 f0 e3 1d a9 15 da a5 6d 1a 8e 72 9f 6b 37 5d ... m r k7

0050 64 93 17 77 8c 27 45 e3 38 39 31 01 4a 07 ... w e s 94 09

0060 50 20 13 fc be 4d b4 5b ad ff 3d 23 ad dc 54 40 ... M [ ... s - TH

0070 15 3a 04 b9 97 5b 0b bc a7 70 32 f4 97 05 04 ... [ ... ] 28 7

0080 0f 45 00 24 13 01 13 03 12 02 c9 2b c9 2f cc a9 ... E S ... / -

0090 00 20 13 fc be 4d b4 5b ad ff 3d 23 ad dc 54 40 ... M [ ... s - TH

00a0 03 77 35 07 32 83 e5 3c 75 07 c5 32 17 5c a0 76 ... u ... u 2 \ v

00b0 04 50 0d 32 87 07 c3 38 00 c8 f0 02 03 c2 f0 ... Y 2 - 8 - p

00c0 00 20 13 fc be 4d b4 5b ad ff 3d 23 ad dc 54 40 ... M [ ... s - TH

00d0 15 3a 04 b9 97 5b 0b bc a7 70 32 f4 97 05 04 ... [ ... ] 28 7

00e0 0f 45 00 24 13 01 13 03 12 02 c9 2b c9 2f cc a9 ... E S ... / -

00f0 00 20 13 fc be 4d b4 5b ad ff 3d 23 ad dc 54 40 ... M [ ... s - TH

0100 cc a8 c0 2c c0 38 c0 0a c0 09 c0 13 c0 14 00 9c ... 0 ...

Cipher Suite (tls.handshake.ciphersuite), 2 bytes Packets: 5244 · Displayed: 52 (1.0%) · Dropped: 0 (0.0%) Profile: Default

ActivitiesApplicationsTerminalSun May 30 20:49

FileEditViewGoCaptureAnalyzeStatisticsTelephonyWirelessToolsHelp

ssh

No.	Time	Source	Destination	Protocol	Length	Info
1878	4.810113621	141.85.241.99	192.168.1.101	SSH	102	Server: Encrypted packet (len=36)
1879	4.912152988	192.168.1.101	141.85.241.99	SSH	102	Client: Encrypted packet (len=36)
1879	4.917411835	141.85.241.99	192.168.1.101	SSH	102	Server: Encrypted packet (len=36)
2030	5.048931061	192.168.1.101	141.85.241.99	SSH	102	Client: Encrypted packet (len=36)
2041	5.057461587	141.85.241.99	192.168.1.101	SSH	110	Server: Encrypted packet (len=44)
2076	5.127655127	141.85.241.99	192.168.1.101	SSH	242	Server: Encrypted packet (len=176)
2076	5.127795763	192.168.1.101	141.85.241.99	SSH	102	Client: Encrypted packet (len=36)
2079	5.127819406	192.168.1.101	141.85.241.99	SSH	126	Client: Encrypted packet (len=69)
4116	8.142234188	192.168.1.101	141.85.241.99	SSHv2	107	Client: Protocol (SSH-2.0-OpenSSH 8.2p1 Ubuntu-4ubuntu1)
4143	8.166533908	192.168.1.101	141.85.241.99	SSHv2	150	Client: Key Exchange Init
4144	8.168822258	141.85.241.99	192.168.1.101	SSHv2	1346	Server: Key Exchange Init
4149	8.173570519	192.168.1.101	141.85.241.99	SSHv2	114	Client: Diffie-Hellman Key Exchange Init
4153	8.184643355	141.85.241.99	192.168.1.101	SSHv2	430	Server: Diffie-Hellman Key Exchange Reply, New Keys, E
4157	8.189090327	192.168.1.101	141.85.241.99	SSHv2	82	Client: New Keys
4186	8.233790729	192.168.1.101	141.85.241.99	SSHv2	110	Client: Encrypted packet (len=44)
4196	8.239338087	141.85.241.99	192.168.1.101	SSHv2	110	Server: Encrypted packet (len=44)
4191	8.239317948	192.168.1.101	141.85.241.99	SSHv2	142	Client: Encrypted packet (len=76)
4219	8.257681251	141.85.241.99	192.168.1.101	SSHv2	634	Server: Encrypted packet (len=568)

Frame 4149: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface vld01, id 0

Ethernet II, Src: Tp-LINKT-99:02:50 (98:90:00:99:02:50), Dst: AzureWav\_e5:70:65 (dc:f5:05:e5:70:65)

Internet Protocol Version 4, Src: 141.85.241.99, Dst: 192.168.1.101

Transmission Control Protocol, Src Port: 22, Dst Port: 49172, Seq: 1, Ack: 42, Len: 21

SSH Protocol

Protocol: SSH-2.0-OpenSSH 7.4

[Direction: Server->Client]

0000 dc f5 05 e5 70 65 98 de 90 f9 82 50 00 00 45 00 ..ve...P.E

0010 00 49 29 08 40 00 34 06 dc 10 8d 55 f1 63 c0 a0 I)04..Uc

0020 01 65 00 16 c0 14 9f 73 27 8a 69 f4 f6 f6 89 10 e...s'.i...

0030 00 e3 30 0a 00 01 00 0a cf 0f 0e 0e 74 b1 0 0...nt

0040 01 51 53 53 48 20 32 2e 30 2d 4f 70 65 0e 53 53 QSSH-2.0-OpenSSH

0050 48 9f 37 2e 34 00 0a H\_7.4..

Message direction (ssh.direction)

vlad\_cristian.matei@fep7-1:-

vlad@vladutz: ~/Desktop/Se... vlاد\_cristian.matei@fep7-1:- vlاد@vladutz: ~/Desktop/Se...

\* Your sessions will be disconnected automatically after 60min on inactivity.  
You can use "-o ServerAliveInterval 10" option if you need longer sessions.\*  
vlاد\_cristian.matei@fep7-1:-\$ sudo ssh vlad\_cristian.matei@fep7-1:-\$  
[sudo] password for vlad:  
The authenticity of host 'fep7-1:- (141.85.241.99)' can't be established.  
ECDSA key fingerprint is SHA256:ks0T8HklipjF70e45QL0aaVwkpPEw07LKwwK13yU.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added 'fep7-1:-,141.85.241.99' (ECDSA) to the list of known hosts.  
vlاد\_cristian.matei@fep7-1:-\$  
\* IMPORTANT - PLEASE READ CAREFULLY:  
\* Inceputand cu 22.09.2019 toate directoarele studentilor vor fi sterse. Va rugam sa va salvati fisierele r  
elevante pana atunci.  
\* If you are using GPU computing and TensorFlow technology, please use CUDA\_VISIBLE\_DEVICES  
to limit the number of GPUs. Otherwise, you will be banned.  
\* Your sessions will be disconnected automatically after 60min on inactivity.  
You can use "-o ServerAliveInterval 10" option if you need longer sessions.\*  
vlاد\_cristian.matei@fep7-1:-\$  
Permission denied, please try again.  
vlاد\_cristian.matei@fep7-1:-\$  
Permission denied, please try again.  
vlاد\_cristian.matei@fep7-1:-\$  
Last failed login: Sun May 30 20:46:34 EEST 2021 from 192.168.6.10 on ssh:ntty  
There were 2 failed login attempts since the last successful login.  
Last login: Sat Feb 1 10:14:12 2020 from 192.168.6.10  
[vlاد\_cristian.matei@fep7-1 ~]\$ ls  
[vlاد\_cristian.matei@fep7-1 ~]\$ pwd  
/export/home/acs/stud/v/vlad\_cristian.matei  
[vlاد\_cristian.matei@fep7-1 ~]\$ ^C  
[vlاد\_cristian.matei@fep7-1 ~]\$ ^C  
[vlاد\_cristian.matei@fep7-1 ~]\$ exit  
logout  
Connection to fep7-1:- closed.  
vlاد@vladutz:~/Desktop/Se...\$  
\* IMPORTANT - PLEASE READ CAREFULLY:  
\* Inceputand cu 22.09.2019 toate directoarele studentilor vor fi sterse. Va rugam sa va salvati fisierele r  
elevante pana atunci.  
\* If you are using GPU computing and TensorFlow technology, please use CUDA\_VISIBLE\_DEVICES  
to limit the number of GPUs. Otherwise, you will be banned.  
\* Your sessions will be disconnected automatically after 60min on inactivity.  
You can use "-o ServerAliveInterval 10" option if you need longer sessions.\*  
vlاد\_cristian.matei@fep7-1:-\$  
Last login: Sun May 30 20:46:39 2021 from 192.168.6.10  
[vlاد\_cristian.matei@fep7-1 ~]\$ pwd  
/export/home/acs/stud/v/vlad\_cristian.matei  
[vlاد\_cristian.matei@fep7-1 ~]\$ ^C  
[vlاد\_cristian.matei@fep7-1 ~]\$ exit  
[vlاد\_cristian.matei@fep7-1 ~]\$