**Lab–Certificate Authority Stores**

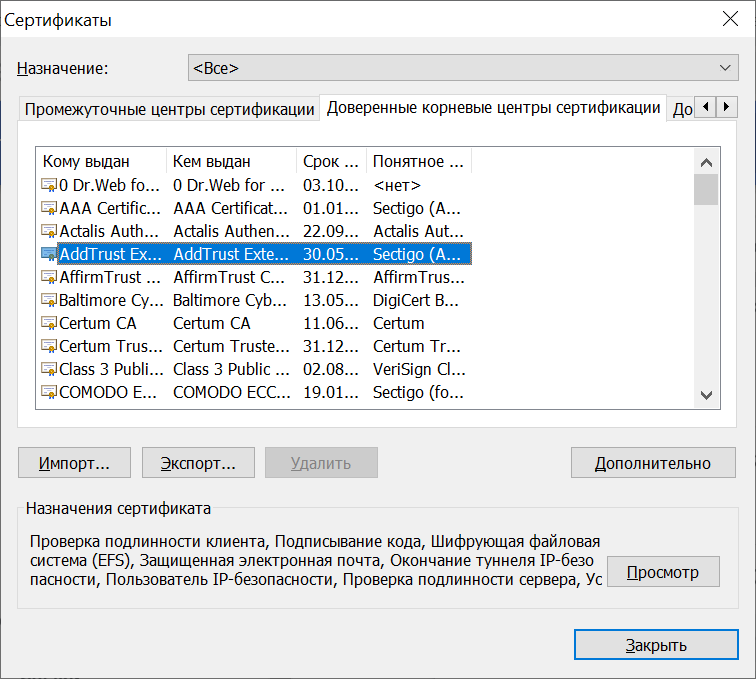
**Objectives**

**Part 1:Certificates Trusted byYour Browser**

**Part 2: Checking for Man-In-Middle**

**Part 1:Certificates Trusted byYour Browser**

Trusted root certification authorities



**Part 2:Checking for Man-In-Middle**

**Step 1:Gatheringthe correctand unmodifiedcertificatefingerprint.**

**What are the fingerprints? Why are they important?**

Fingerprinting happens when sites force your browser to hand over innocent-looking but largely unchanging technical information about your computer, such as the resolution of your screen, your operating system or the fonts you have installed. Combined, those details create a picture of your device as unique as the skin on your thumb.

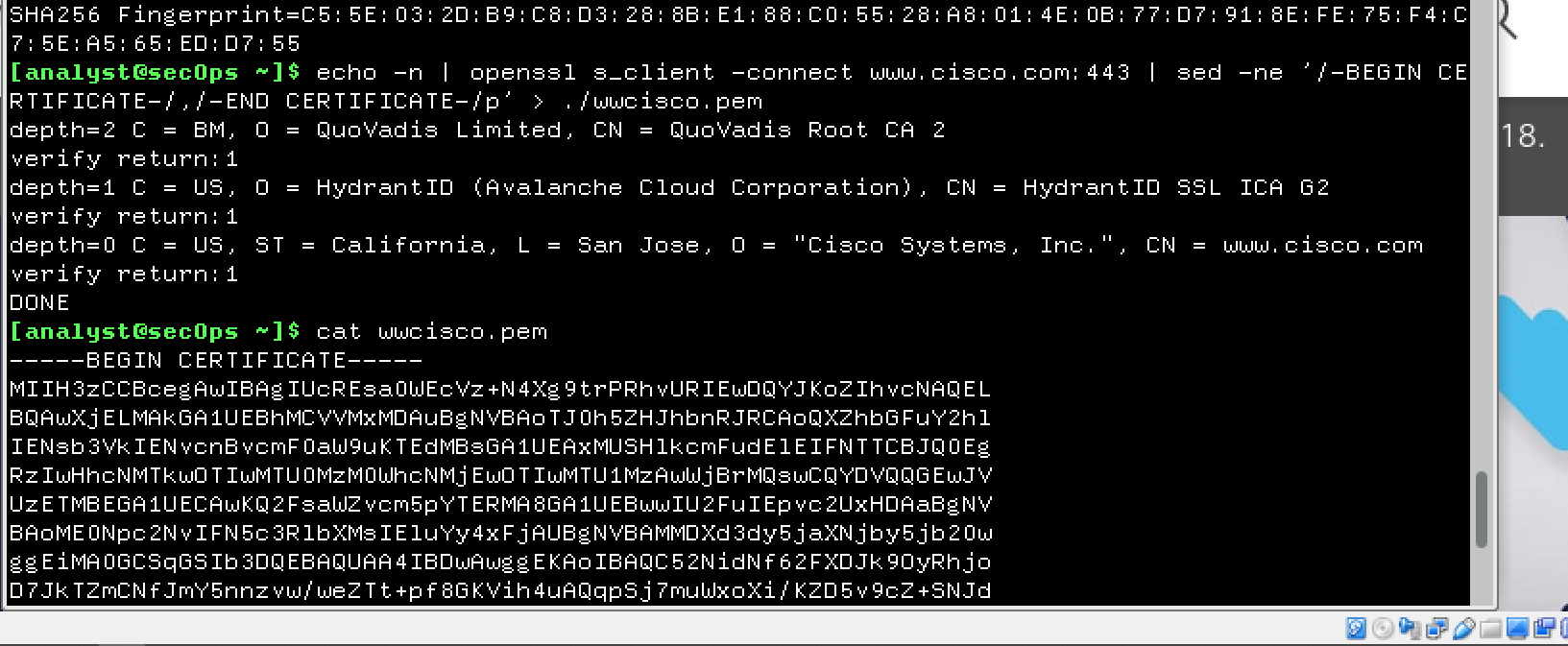
Sites can use your digital fingerprint to know if you’ve visited before, create profiles of your behavior or make ads follow you around. They can also use it to stop you from sharing a password, identify fraudsters and block harmful bots.

**Who calculates fingerprints? How to find them?**

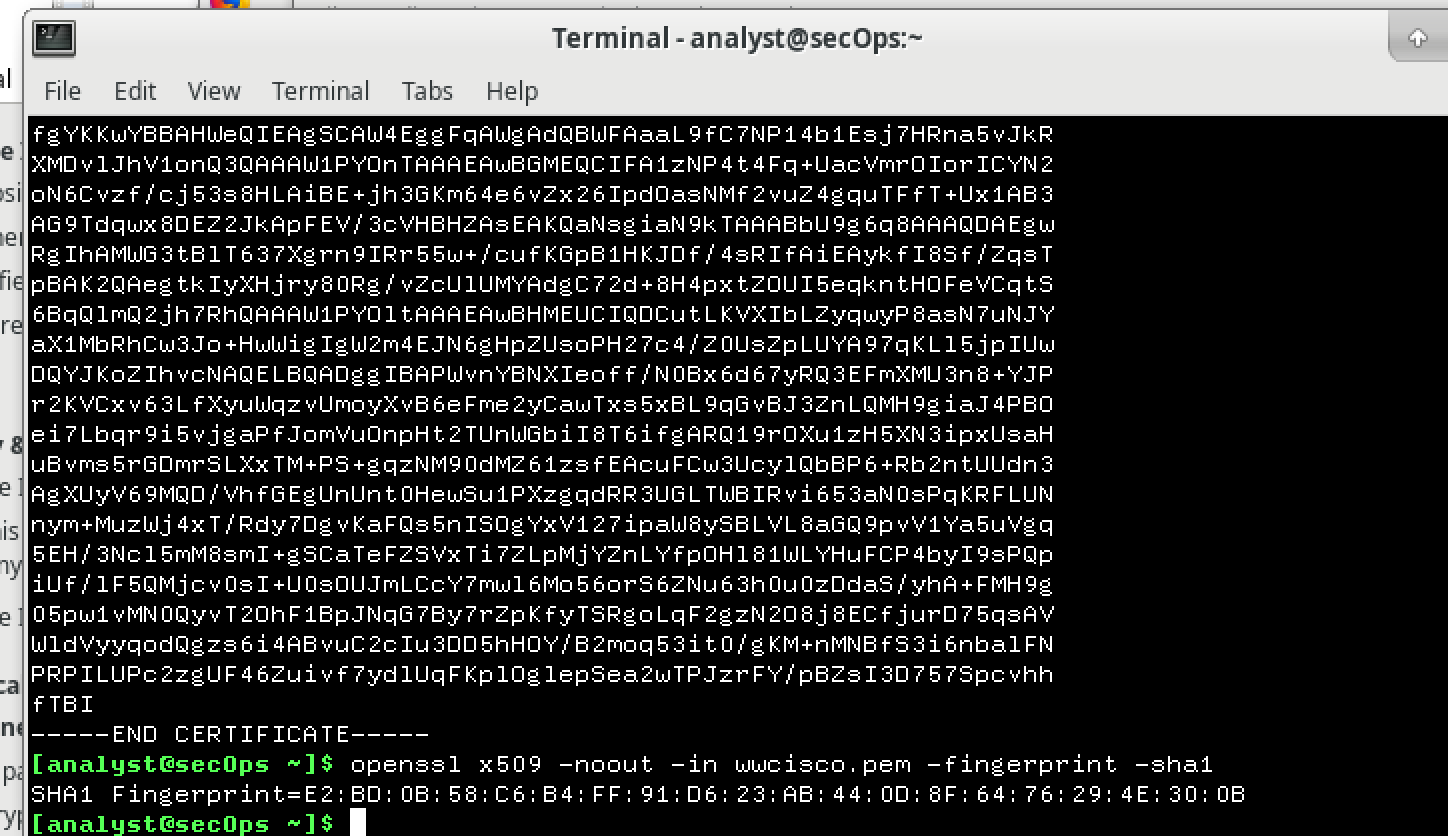
The certificate fingerprint is usually calculated by the CA that signs the certificate. After it has been computed, the CA includes it in the certificate itself. The fingerprint can be easily displayed when viewingthe certificate.

Step 2:Gather the certificate fingerprint in use by the CyberOpsWorkstation VM.

1. Cisco.pem certificate



1. Extract certificate fingerprint



1. What hash algorithm was used by OpenSSL to calculate the fingerprint?  
   SHA-1
2. Why was that specific algorithm chosen? Does it matter?

It is not so matter, because these fingerprints are not actual in 2020. But it will be matter if websites not update their fingerprints. In that case we be able to compare our sha1 fingerprint with the sha1 fingerprints in table. So for checking is it right fingerprint it is matter to use sha1 as in table. In my case I compared it with fingerprint by Browser GUI method.

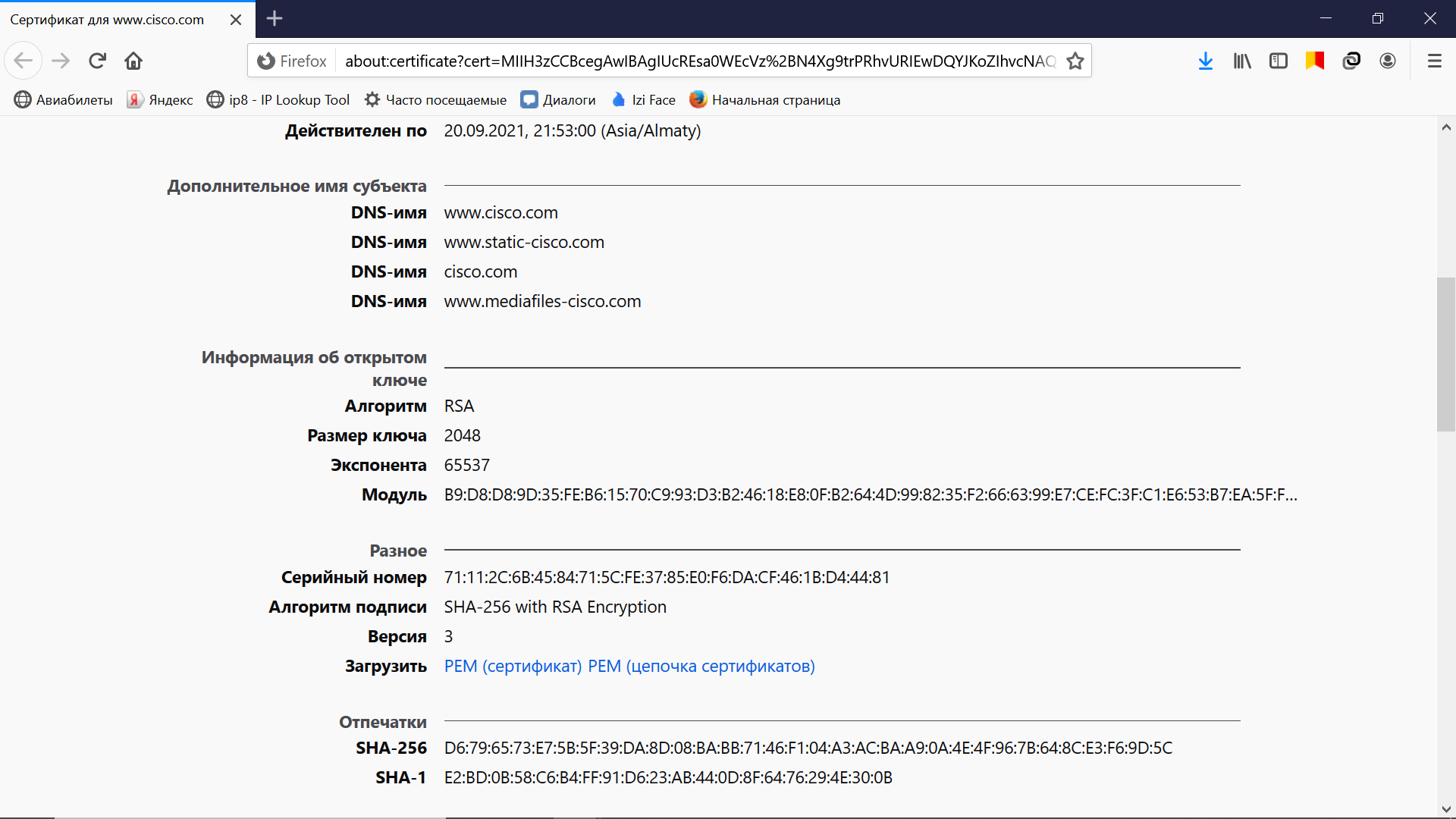
**Step 3:Compare the Fingerprints**

Do the fingerprints match?

They are not match

What doesit mean?

Fingerprint which I get use different from the table, but it matches with the fingerprint in website. It means fingerprint was updated in 2020



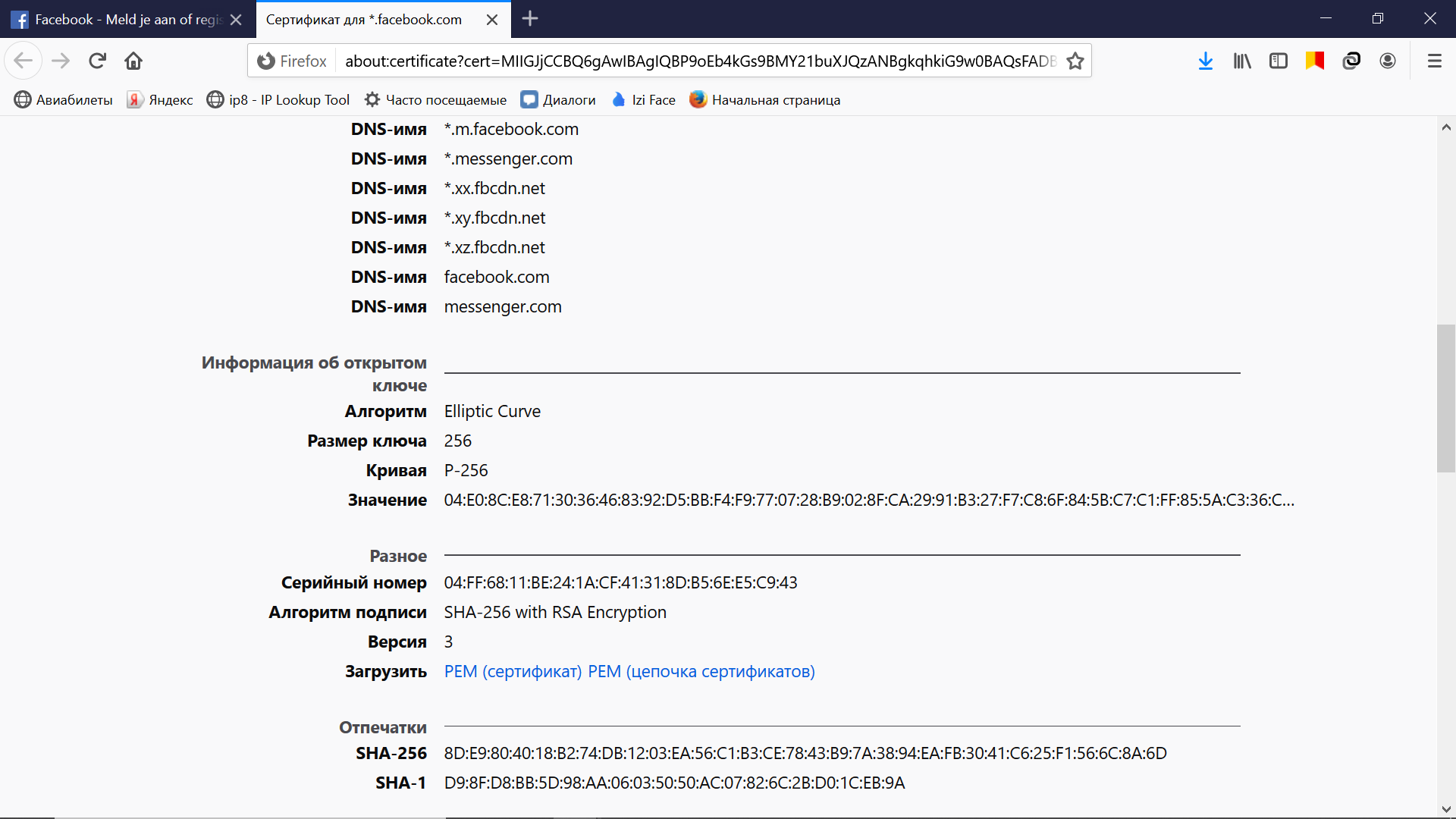
While if it differce from the cisco certificate it means that someone intercepted the connection and send a new SSL/TLS certificate.

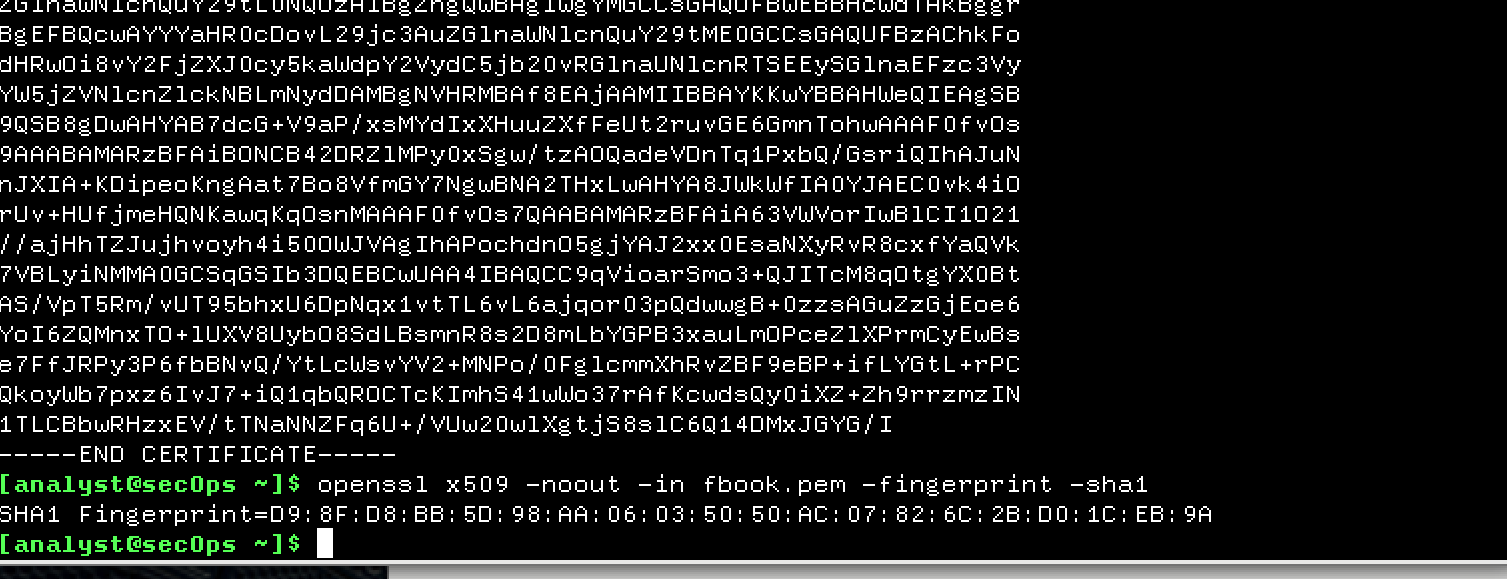
Is this method 100% foolproof?

No, VM will not have any enterprise-owned CA root certificates installed. It means VM may not have its traffic intercepted, but it can be done for the local network machines. The enterprise could use dynamic rules to intercept only selected sites.

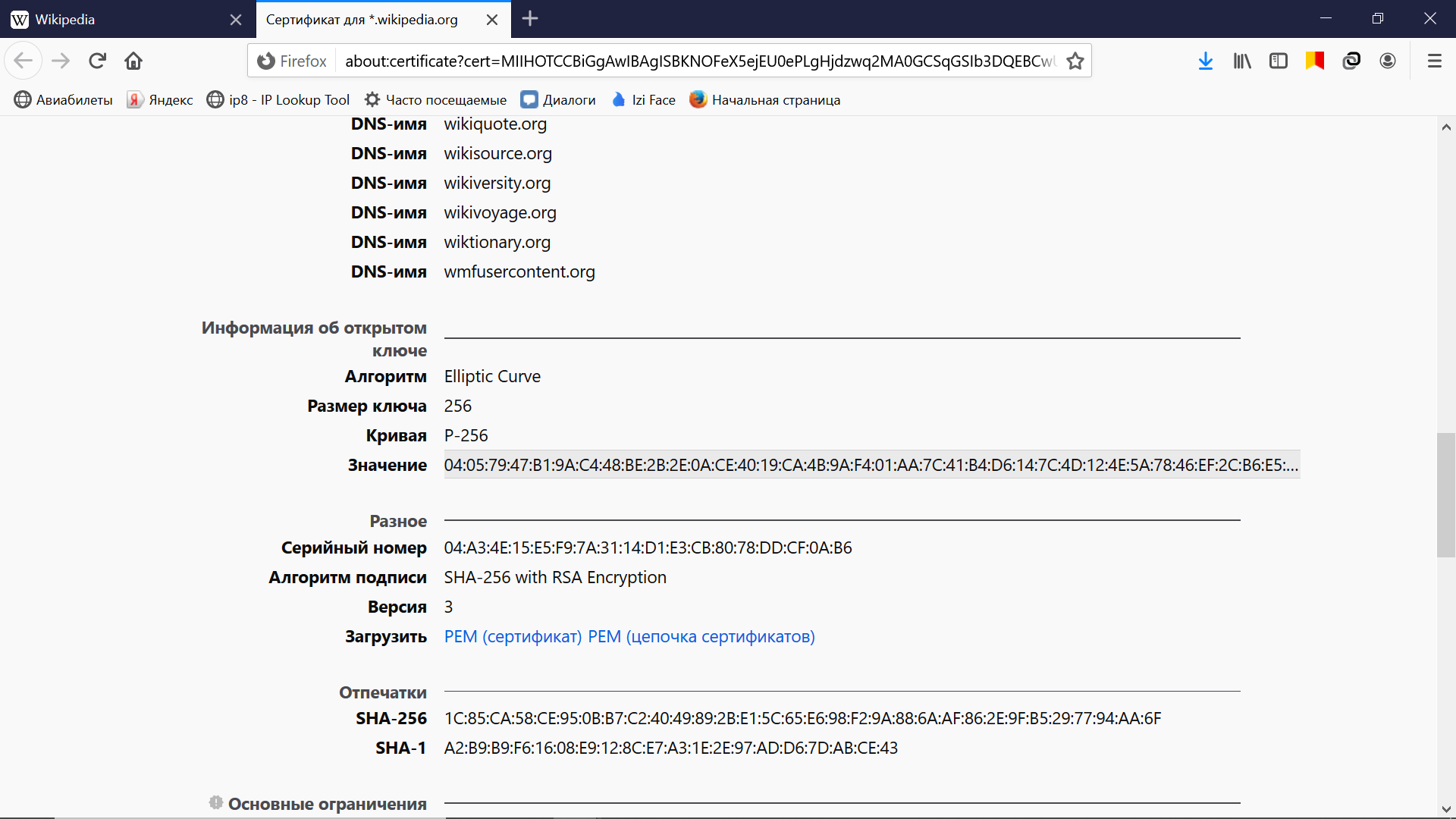
**Part 3:Challenges(Optional)**

www.facebook.com



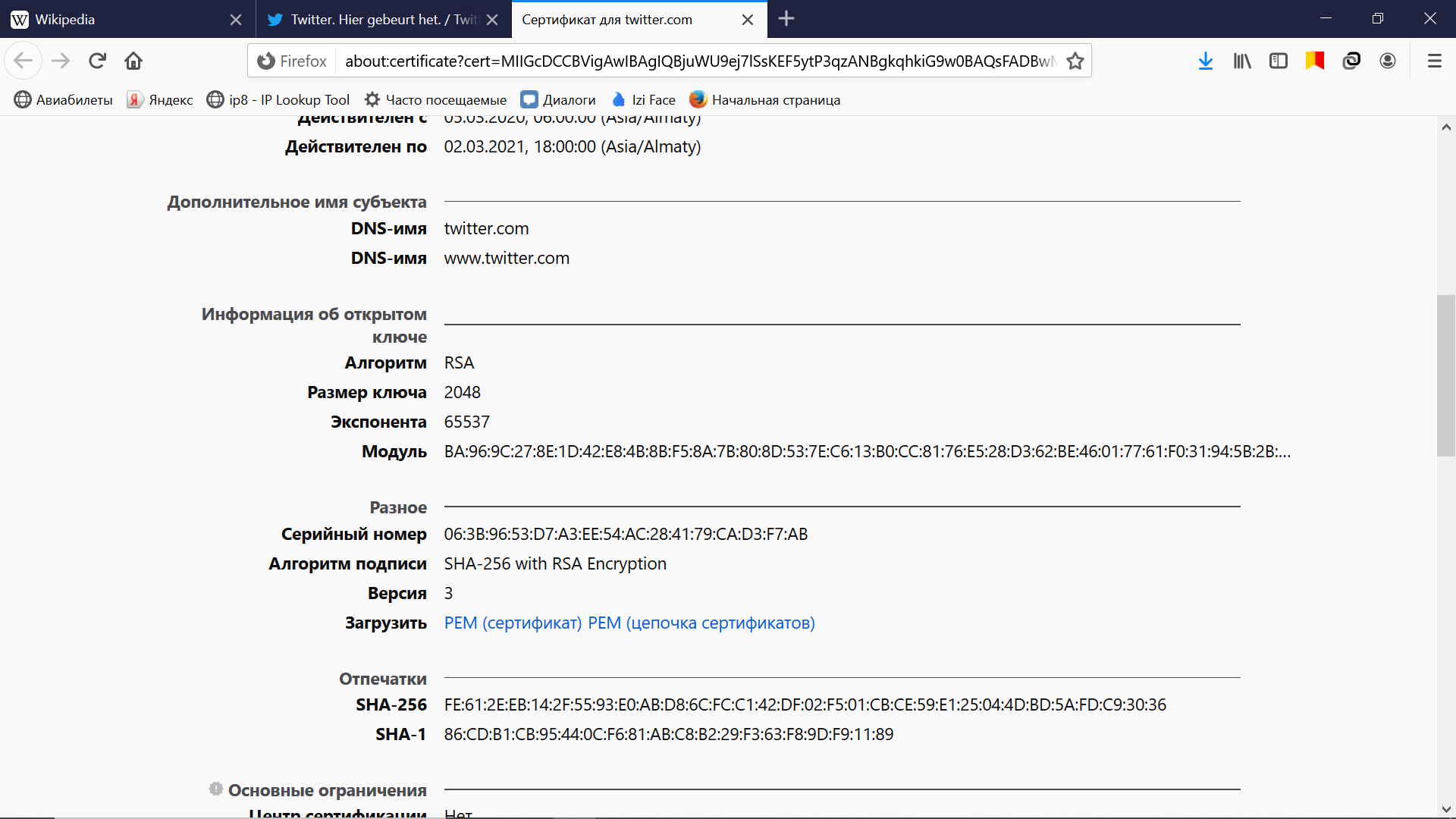


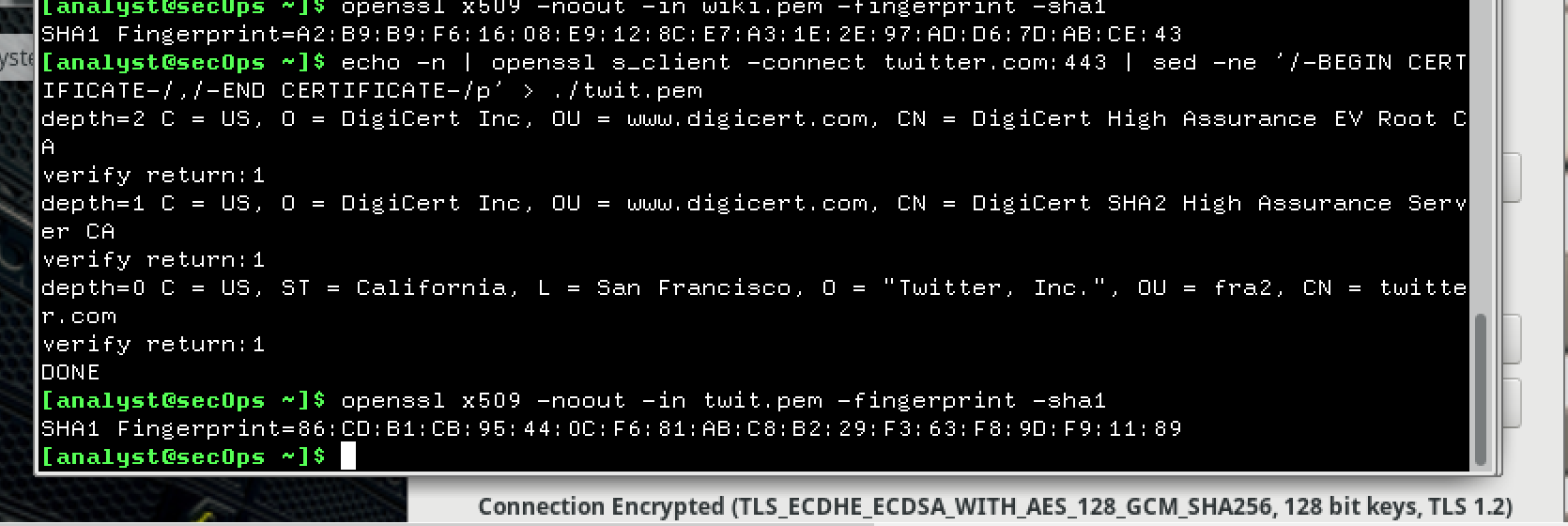
[www.wikipedia.org](http://www.wikipedia.org)



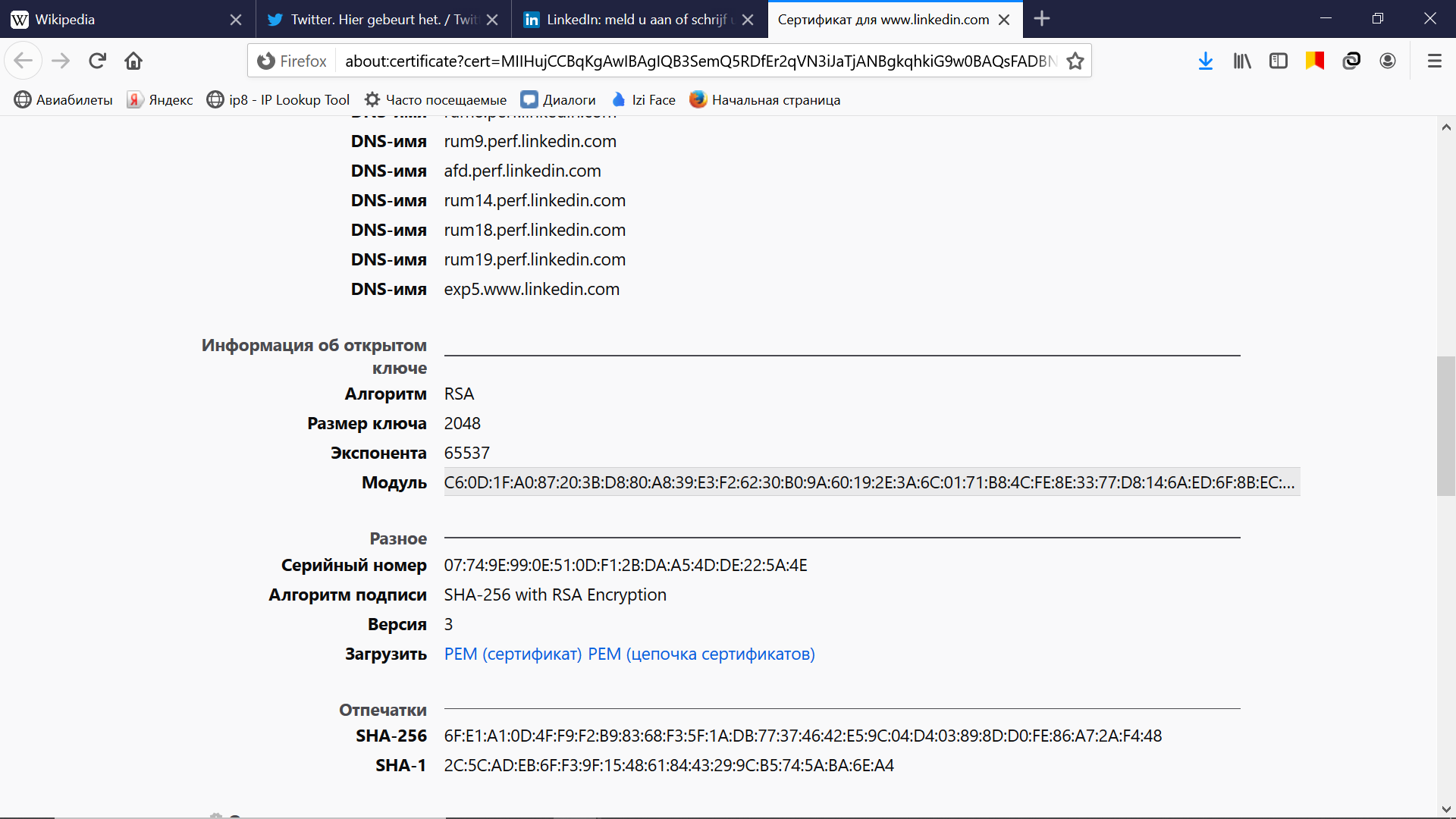


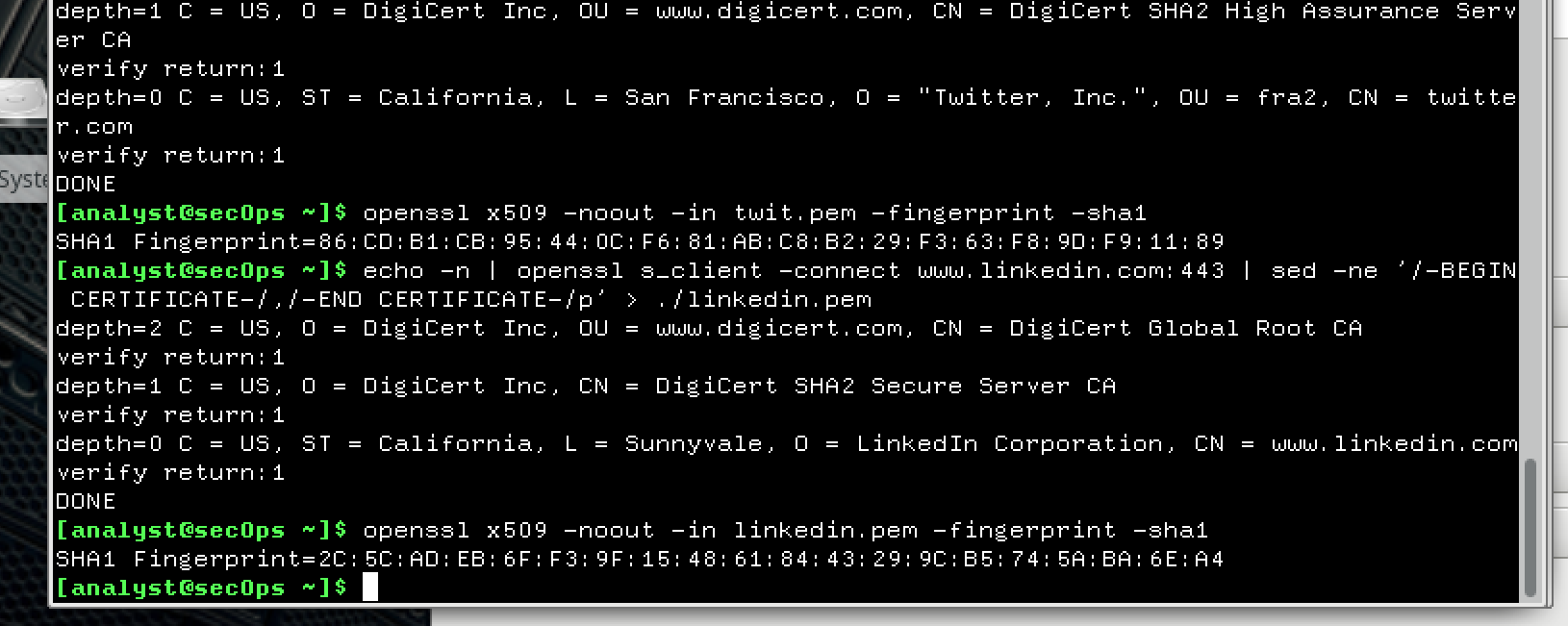
Twiter.com





[www.linkedin.com](http://www.linkedin.com)





What would be necessary for the HTTPS proxy to work?

Local machine should fully trust to HTTPS proxy. It achieves by installing the HTTPS proxy’s certificate into the local machine’s root certificate store. It allow to decrypt the traffic without warnings.