Debookee Documentation

Release

iwaxx Sàrl

Jan 25, 2018

Contents

Debookee is a simple and powerful network traffic analyzer for macOS.

https://debookee.com

CHAPTER 1

Introduction

Debookee is a simple and powerful network traffic analyzer for macOS.

https://debookee.com

CHAPTER 2

Installation

2.1 Installation on macOS

- The minimum macOS version is 10.10
- Download the last stable version of Debookee from https://debookee.com.

2.2 Beta installations

First download the last stable version from https://debookee.com.

Then launch Debookee and go in the following menus:

```
Debookee -> Preferences... -> General -> Propose beta version updates: **Checked**
Debookee -> Check for Updates...
```

2.3 Other OSes

Debookee can't be used on other OSes than macOS.

There's no development for Windows & Linux platforms scheduled.

It can't be developped for mobiles (iPhone / iPad / Android) due to low-level permissions to handle network traffic. (This would require jailbreaking/rooting)

CHAPTER 3

LanScan

LanScan is a Layer 2 & Layer 3 network scanner which discovers network devices thanks to ARP, ICMP, DNS, mDNS and SMB packets.

3.1 Scanning local LAN

By default, LanScan scans your local LAN and scanned IPs are configured following your network configuration (IP address and network mask).

```
Your Mac IP address : 192.168.1.10
Your Mac Netmask    : 255.255.255.0 or /24
Exampes of local scans:
     -> From 192.168.1.1 to 192.168.1.254
     -> From 192.168.1.15 to 192.168.1.20
```

A local scan will allow you to:

- Discover MAC addresses of devices
- Set a custom hostname to each device
- Set a custom comment to each device
- Select a device as a *Target*
- Select a device as a *Gateway*

3.2 Scanning external IP ranges

If you modify LanScan IP range to IPs which do not belong to your local LAN, LanScan will make an external scan with only ICMP packets (Layer 3 packets). ARP packets (Layer 2 packets) are not available as packets have to cross over a router to reach destinations IPs.

An external range can be done with private or public IPs,

```
Your Mac IP address : 192.168.1.10
Your Mac Netmask    : 255.255.255.0 or /24
Examples of external ranges:
    -> From 192.168.0.1 to 192.168.0.254
    -> From 10.10.50.10 to 10.10.50.20
    -> From 8.8.8.8 to 8.8.8.8
    -> From 1.0.0.0 to 190.0.0.0
```

An external scan have the following limitations:

- You can't see MAC addresses of devices
- You can't set a custom hostname
- You can't set a custom comment
- You can't select a device as a *Target*
- You can't select a device as a *Gateway*

CHAPTER 4

Traffic Interception (MITM)

Debookee is able to intercept the traffic of any device in the same subnet, thanks to a Man-in-the-middle attack (MITM).

It intercepts all network traffic happening between *Targets* and a *Gateway*. This traffic is then analyzed by the *NA — Network Analysis Module*.

It allows you to transparently capture data from mobile devices on your Mac (iPhone, iPad, Android, BlackBerry…) or Printer, TV, Fridge… without setting any proxy.

Note: Interception is a native feature of Debookee, included in the free trial.

You don't need the NA license to intercept targets traffic to your Mac, but the results of analysis (HTTP, TCP …) will be obfuscated at some point in the free trial of NA module.

> **Warning:** **Interception may fail** on some networks, specially on professional wireless networks (Aruba, Cisco, HP…), due to Proxy ARP or security features that detect the MITM.
>
> In that case, you won't see any traffic under your target menu. A workaround can be to set up a mobile hotspot or connect to another network.
>
> We recommend to always try the free trial of *NA Module* to check if your network allows network traffic interception or not before buying it.

4.1 Target

Debookee intercepts all network traffic between Targets and the configured *Gateway*.

You can set as many Targets as you want, but they must be on the same subnet as your Mac, as we need to know their MAC addresses. (cf *Scanning local LAN*)

To set a Target:

- Stop the NA module if already running
- Select a device which has no role & located on the same LAN
- Click on “Toggle Target” or double-click on the device ‘role’ column

4.2 Gateway

A Gateway is the device to which *Targets* are talking to and you’re interested in that traffic.

You can set only one Gateway.

By default, the Gateway is set to the *default gateway* or *router* of your Mac network interface. So by default, if you set a Target, you’ll intercept the traffic from the Target to the router, ie the Internet traffic.

One reason to modify the Gateway from the router to another device on your network is if you want to intercept some internal network traffic on your LAN.

If you’re interested in the traffic between your iPhone and your printer, both located on your LAN:

- Set your iPhone as a Target
- Set your printer as a Gateway
- (Note that Debookee won’t see your iPhone Internet traffic in that case.)

To set a Gateway:

- Stop the NA module if already running
- Select a device which has no role & located on the same LAN
- Click on “Set Gateway”

CHAPTER 5

Trial Limitations

For all modules, trial demo and licensed versions contain **exactly the same features**, only some results are **obfuscated** in the demo.

Using the free trial, at some point, you may see such obfuscations with `*** Trial Evaluation ***`

```
15:47:17    http://ssl*** Trial Evaluation ***      GET     200 OK  application/x-
↪font-woff 5.4 kB
    GET /pla*** Trial Evaluation ***
    Host: ssl*** Trial Evaluation ***
    Connection: kee*** Trial Evaluation ***
    User-Agent: Moz*** Trial Evaluation ***
    Origin: htt*** Trial Evaluation ***
    Accept: */**** Trial Evaluation ***
    Referer: htt*** Trial Evaluation ***
    Accept-Encoding: gzi*** Trial Evaluation ***
    Accept-Language: fr-*** Trial Evaluation ***
    DNT: *** Trial Evaluation ***
```

Licensing a module will simply deobfuscate the text.

Warning: Don't buy a license thinking that this will "unblock" features or let missing results appear.

If results are not the expected ones (missing devices in LanScan, missing results in protocols in NA module, no results at all for a target), licensing the module won't show you *new* results. Contact the support in that case to understand what's wrong.

CHAPTER 6

NA — Network Analysis Module

6.1 NA Module

The NA module analyzes in real-time the network traffic of your own Mac and *intercepted targets*.

It currently supports:

- HTTP
- DNS
- TCP
- DHCP
- SIP & RTP (VoIP) protocols.

6.2 Raw packets of your targets with Wireshark

Some users need more details (or raw data) and use Wireshark for their own traffic. Unfortunately, Wireshark can't intercept traffic like Debookee does, and they can't see their iPhone/Android/Fridge/... raw data.

One idea is to use both Debookee and Wireshark at the same time:

- Find and select your target with LanScan
- Launch the NA module to start the interception, but ignore the NA results
- Start Wireshark on your Mac: you'll see your own traffic as well as the intercepted target's traffic

---

Tip: For each packet, Wireshark will see the packets coming to your Mac, and the same packet retransmitted transparently by the Mac. Target's traffic in that case will be doubled in Wireshark and you'll see all packets **duplicated**.

To filter, one idea of display filter could be to hide all outgoing packets of your targets like: `!(eth.src == mac_address_of_my_mac && ip.src != ip_of_my_mac) && !(eth.dst == mac_address_of_my_mac && ip.dst != ip_of_my_mac)`

CHAPTER 7

WM - Wi-Fi Monitoring Module

7.1 WM module

The Wi-Fi Monitoring module puts your airport interface in monitoring mode and listens to all 802.11 radio frames around.

It currently shows you:

- Access Points radio details in your radio range
- Wi-Fi clients radio details in your radio range
- Informations on clients association (useful to detect roaming or when multiple AP with same SSID)
- Bidirectional infos for each client connection: from AP to client and client to AP
  - Data Rate
  - %Retries
  - %Errors
  - Bytes transferred
  - Channels stats
  - Power signal in dBm
  - ...

For those asking, WM module can't decrypt encrypted packets of other Wi-Fi networks.

7.2 Differences with NA module

Starting WM module sets your Mac Wi-Fi interface in monitoring mode. (which is different than *promiscuous*, see this article)

Monitoring mode has the following consequences:

- Your Wi-Fi interface will be directly disconnected
- You will loose all network connectivity
- You see all *radio* packets, even the Wi-Fi packets of your neighbor (encrypted or not)
- WM module doesn't care if packets are encrypted: it shows you radio statistics, not content analysis

CHAPTER 8

SSL — SSL/TLS Decryption Module

Note: SSL module is currently only available in beta and for *macOS 10.12 minimum.* You can enable beta updates inside Debookee in `Menu Debookee -> Preferences -> General -> Propose beta version updates` Then force update with `Menu Debookee -> Check for Updates...`

Check out this blog post for more informations.

The SSL module is an extension of *NA Module* which allows HTTPS decryption of your own traffic and *intercepted targets* by setting an HTTPS man-in-the-middle proxy.

By default, TLS decryption is not enabled. Debookee can run in 3 modes:

- No TLS decryption
- TLS decryption for targets only
- TLS decryption for Own Traffic and all the intercepted targets

8.1 How it works

1. We intercept the client HTTPS connection (*Client->Debookee*)
2. Create it's own HTTPS connection to the server (*Debookee->Server*)
3. Retrieve some data from the server & decrypt them
4. Create on-the-fly a fake certificate impersonating the server, created from Debookee's Certificate Authority (CA)
5. Send the fake certificate to the client and establish *Client->Debookee* TLS connection
6. Send the data to the client

8.2 Clients SSL/TLS warnings/failures

Most HTTPS clients (browsers, applications, email clients. . .) will detect Debookee's fake certificates and will behave differently, depending their capabilities.

A solution to avoid those warnings can be the *installation of Debookee's Certificate Authority* on the client.

By default, without Debookee's CA, reactions to the fake certificate could be:

1. Clients present a warning and propose to accept the fake certificate
2. Clients present a fatal alert and deny the connection in case of Key Pinning
3. Clients TLS connections fails silently

8.2.1 Examples

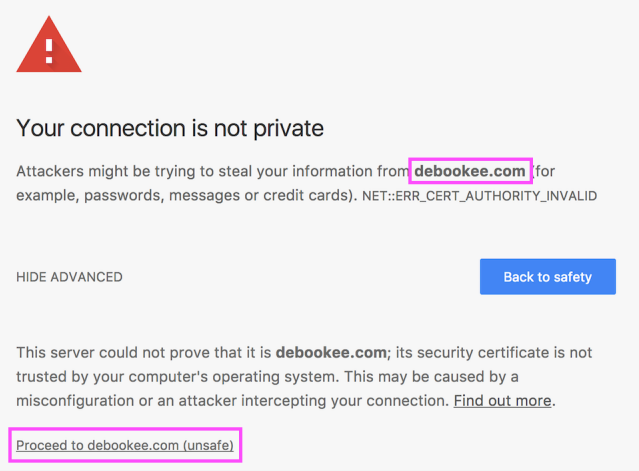


Fig. 8.1: CA certificate is not installed on client and debookee.com doesn't implement Key Pinning -> Chrome proposes you to proceed with fake certificate

8.3 Key Pinning

Some clients implement HTTP Public Key Pinning, a security mechanism which prevents impersonation of a TLS server.

Key Pinning can be strict or not. When strict, even if the CA is installed, the client won't accept to establish the impersonated TLS connection. In a future release, Debookee will implement a white-list to avoid decryption of some connections involving strict Key Pinning.

8.4 Installation of Debookee's Certificate Authority (CA)

8.4.1 Target traffic decryption

If you intercept a target traffic and want to decrypt its traffic, by default, the client's browser will warn you of the MITM attempt. In that case, you need to install the Debookee's Certificate Authority on the target (not on the Mac

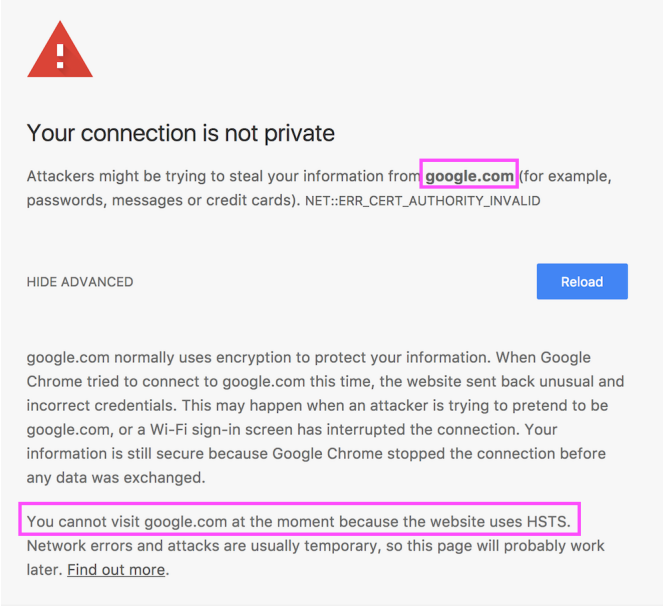
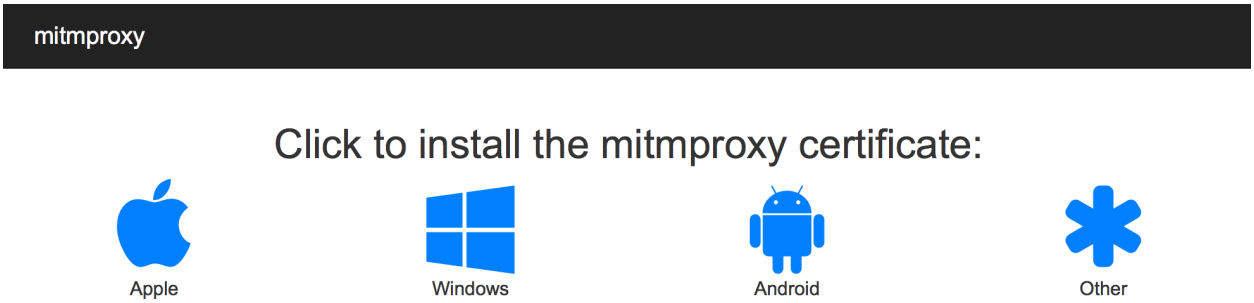


Fig. 8.2: CA certificate is not installed on client and google.com uses Key Pinning -> no way to access the website

running Debookee).

You can access the certificate with the following steps:

1. Select a target
2. Start NA module, target's traffic must be intercepted
3. On the target, run a browser on `http://mitm.it:6969`
4. Follow the steps on the following website to install the CA on the target



The webpage is proposed by mitmproxy which is internally used in Debookee for the SSL/TLS decryption. If you want to learn more about this incredible project, you can checkout their very complete documentation..

8.4.2 Own Traffic decryption

To decrypt your Own Traffic without browser's warnings, you need to install the CA on the Mac running Debookee. You don't need to manually install certificate in the Keychain, this can be done automatically in Debookee by pressing `Add CA cert to Keychain`.

Press `Remove CA cert from Keychain` to disable automatic decryption of your traffic and bring back warnings.

If you need to have access to the certificates for *Private certificate store*, life for targets, you can browse `http://mitm.it:6969` from a browser on the Mac running Debookee.

8.4.3 Private certificate store

Target traffic decryption and *Own Traffic decryption* allows you to install a CA certificate into the system certificate store of the OS. (macOS Keychain, Windows, Android certificate store, etc . . .)

Some applications are not using the OS certificate store, but instead have their own, like Firefox or Thunderbird.

In that case, you will have to install manually Debookee's CA certificate inside the private certificate store. You'll find the CA file by downloading it from `http://mitm.it:6969`.

CHAPTER 9

PRO - Professional Module

Note: PRO module is currently only available in beta and for *macOS 10.12 minimum.* You can enable beta updates inside Debookee in `Menu Debookee -> Preferences -> General -> Propose beta version updates` Then force update with `Menu Debookee -> Check for Updates...`

Check out this blog post for more informations.

PRO module is an extension of the SSL module which implements:

- Email decryption : IMAPs / SMTPs / POP3s decryption of your own traffic and all your targets traffic
- Allows you to create your own Certificate Authority details (Common Name, Organization, etc . . .)
- Allows you to decrypt SSL/TLS on different port than the default (For ex: 8443)

CHAPTER 10

Combos: Buying several modules

You can buy several modules within a combo, which will be less expensive than buying each module independently.

NA+WM	Purchase page
SSL+PRO	Purchase page
NA+SSL	Purchase page
NA+SSL+PRO	Purchase page
NA+WM+SSL	Purchase page
NA+WM+SSL+PRO	Purchase page

CHAPTER 11

Debookee

11.1 Does network traffic interception always work in NA module?

No.

Network Analysis (NA) module allows you to select targets and intercept their traffic through a Man-in-the-middle attack (ARP spoofing).

On wired networks, this will almost always work. We've seen some situations where the traffic was only half intercepted, in that case you'll have only some traffic like only DNS answers, but no requests from your targets.

On professional wireless networks (Aruba, Cisco, HP. . .), this interception will likely fail due to Proxy ARP or security features that detect the MITM. In that case, you won't see any traffic under your target menu. We suggest to set up a mobile hotspot or connect to another network in that case.

We recommend to always try the free trial of Debookee NA module to check if your network allows network traffic interception or not.

11.2 Will you sell Debookee on Mac App Store?

Unfortunately not: the library used to capture packets needs admin privileges, which are forbidden by Mac App Store guidelines.

This elevation of privileges is made following Apple's standard API: at no point will we have knowledge of your password.

11.3 Beta version is buggy, how do I revert to last stable version?

First, please explain us clearly what is going wrong with an email at support@iwaxx.com with some details and screenshots. A beta version is supposed to go in a stable state, and we need to fix bugs. So please help us by reporting problems before using the stable version.

- Go in menu `Help -> Uninstall Packet Capture Tool`
- Delete the beta application
- Download last stable version from https://debookee.com
- Keep checked "Propose beta version updates"!

11.4 What are the limitations of the free trial?

The code is exactly the same: all functionalities are included in the free trial and you can try all of them: interception of traffic, Wi-Fi monitoring, VoIP plugin, SSL decryption, etc…

The only difference is that some results will be obfuscated at some point in the demo version.

You'll need a license to display all results.

11.5 Can I use a VPN connection on the Mac running Debookee?

Currently, Debookee can't handle different interfaces which is the case when a VPN connection is established. (virtual or not)

Packets will be intercepted from ethernet or airport interface and then sent to the gateway/internet through the VPN interface.

But the response packets will be received on the VPN interface (tun, ppp) on which Debookee is not listening too, and thus ignored and dropped.

As a result, intercepted devices will stop working properly.

11.6 I don't need Debookee, I use Wireshark.

We love Wireshark too! So much that we included it in Debookee.

NA & WM modules use Lua scripts & tshark and we worked with Wireshark core dev team during SharkFest 2015 to integrate the whole stuff, while respecting their open source license.

But wait. Don't throw away Debookee directly, if you want to see raw data of your mobiles or IoT things, maybe you'll be interested in *Raw packets of your targets with Wireshark*, because Wireshark alone will show you your own traffic, it can't intercept traffic of other devices on your network like NA module.

11.7 I've installed the certificate on iOS but iPhone/iPad traffic is still not decrypted?

You've correctly *installed the root certificate* on iOS if you see Debookee's certificate in `General -> Profile` on your iPhone/iPad.

Additionally, for iOS version 10.3 and later, you also need to manually enable full trust for that certificate. Make sure Debookee's CA is also enabled in `Settings > General > About > Certificate Trust Settings`

Check out this Apple's FAQ for more information.

CHAPTER 12

LanScan on AppStore

12.1 I've bought LanScan Pro In-App, but free trial always appears?

If In-App is really purchased, this is an App Store issue.

Try to restore the purchase in LanScan: Buy Pro version -> Restore previous purchase

If it doesn't work:

1. Be sure that you're signed into App Store: you must have access to your account without password (Store -> View My Account)
2. Be sure you see your In-App purchase in "Purchased" tab in App Store
3. Did you log in different country in App Store than the country you did the purchase?
4. Try to log out / log in App Store (Store -> Sign Out)

If you have to restore the purchase every time you start LanScan:

1. Try to log out / log in from App Store (Store -> Sign Out)
2. Delete LanScan from your Applications
3. Empty your trash (important, else your Mac still see your app in the trash)
4. Reinstall LanScan free trial from App Store
5. Restore the purchase if needed in LanScan: Buy Pro version -> Restore previous purchase

12.2 What are the differences between LanScan App Store apps and the LanScan tool included in Debookee?

LanScan - Free - App Store	Only 4 hostnames are fully displayed, you'll see the first 3 chars of the others.
LanScan - In-App purchase Pro - App Store	No limitation on resolved hostnames
LanScan Pro	No limitation on resolved hostnames. Same code as In-App purchase, it was just created before In-App existed. Since v4, it's preferred to buy the In-App purchase in LanScan Free edition than buying the LanScan Pro application.
Debookee's LanScan tool	Advanced version of LanScan Pro application. Each new feature is first released in Debookee's LanScan tool, then on App Store

12.3 A MAC address vendor is not resolved in LanScan results.

We're using the IEEE list for our vendors database and currently, we refresh this database on each update of our applications.

As it's updated more frequently, Debookee will typically have a more up-to-date vendors list than LanScan and LanScan Pro. Dynamic updates will be added in a future release.

12.4 Where are custom hostnames located?

At first: *please backup!*

Custom hostnames are saved in the following XML plist files. Take care that those files can be cached, and you may edit them without seeing any results. So please be sure to erase the plist cache with command: `defaults read my_freshly_edited_plist_file.plist`

LanScan	~/Library/Containers/com.iwaxx.LanScan/Data/Library/Preferences/com.iwaxx.LanScan.plist
LanScan Pro	~/Library/Containers/com.iwaxx.LanScan-Pro/Data/Library/Preferences/com.iwaxx.LanScan-Pro.plist
Debookee	~/Library/Preferences/com.iwaxx.Debookee.plist

12.5 Several devices have the same duplicated MAC address but different IPs.

LanScan doesn't modify anything on your network: think about it as Read-Only on your network, it asks questions (ARP requests) and display answers listened directly from the network.

Duplicated MAC addresses are usually cause by a device which is answering instead of other ones, commonly called ARP proxy or "Bonjour Sleep Proxy" in case of Apple devices (Airport Extreme, Time Capsule, Apple TV...)

12.5.1 ARP proxy

Commonly used on wireless network to lower broadcasted traffic, you may see an Access Point (AP) or a router answering instead of other devices, in that case you'll see the AP or router's MAC address duplicated. → If you're scanning while on the Wi-Fi, try to cable your Mac and scan again from the LAN point of view.

12.5.2 Bonjour Sleep Proxy

In short, when an Apple compatible device such as a Mac, an Apple TV... goes in sleep mode, it advertises the Apple device compatible with Bonjour Proxy, which will answer to some requests in its name (including those that LanScan send to discover devices), so that the TV or the Mac stays in sleep mode.

You can find more information here: https://en.wikipedia.org/wiki/Bonjour_Sleep_Proxy

In that case you'll see several time the MAC address of the device acting as a proxy. → Waking up the final device should help to show its real MAC address in that case

CHAPTER 13

Blog