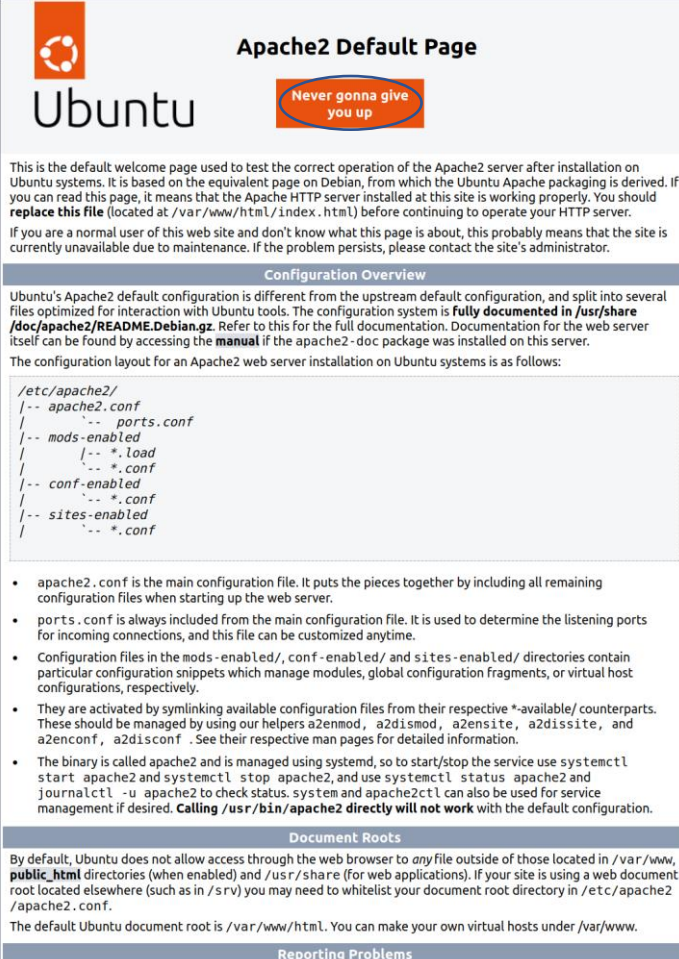


### רשתות תרגיל 3

#### חלק א:

ראשית, התקנתי את הדפדפן, פתחתי את הקובץ `/var/www/index.html` מהטרמינל וכתבתי בו בכותרת "Never gonna give you up" במקום ה"it works".

והרי התוצאה



**Apache2 Default Page**

Never gonna give you up

Ubuntu

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

#### Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective `*-available/` counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2ensite`, `a2dissite`, and `a2enconf`, `a2disconf`. See their respective man pages for detailed information.
- The binary is called `apache2` and is managed using `systemd`, so to start/stop the service use `systemctl start apache2` and `systemctl stop apache2`, and use `systemctl status apache2` and `journalctl -u apache2` to check status. `system` and `apache2ctl` can also be used for service management if desired. **Calling `/usr/bin/apache2` directly will not work** with the default configuration.

#### Document Roots

By default, Ubuntu does not allow access through the web browser to *any* file outside of those located in `/var/www/`, `public_html` directories (when enabled) and `/usr/share` (for web applications). If your site is using a web document root located elsewhere (such as in `/srv`) you may need to whitelist your document root directory in `/etc/apache2/apache2.conf`.

The default Ubuntu document root is `/var/www/html`. You can make your own virtual hosts under `/var/www`.

#### Reporting Problems

כעת, הרצתי מאותו המחשב לקבלת והסנפתי את התעבורה, ספיצפתי (מלשון ספציפי) עם `tcp.port==80`, וקיבלתי:

	Info	Length	Protocol	Destination	Source	Time
...	Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM Tsv [SYN]	80 → 49686 74	TCP	185.125.190.18	192.168.254.129	0.000000000 1
	Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 [SYN, ACK]	49686 → 80 58	TCP	192.168.254.129	185.125.190.18	0.005066000 2
	Seq=1 Ack=1 Win=64240 Len=0 [ACK]	80 → 49686 60	TCP	185.125.190.18	192.168.254.129	0.005690000 3
	GET / HTTP/1.1 141		HTTP	185.125.190.18	192.168.254.129	0.006158000 4
	Seq=1 Ack=88 Win=64240 Len=0 [ACK]	49686 → 80 54	TCP	192.168.254.129	185.125.190.18	0.006384000 5
	HTTP/1.1 204 No Content 201		HTTP	192.168.254.129	185.125.190.18	0.133931000 6
	Seq=148 Ack=88 Win=64240 Len=0 [FIN, PSH, ACK]	49686 → 80 54	TCP	192.168.254.129	185.125.190.18	0.134495000 7
	Seq=88 Ack=148 Win=64093 Len=0 [ACK]	80 → 49686 60	TCP	185.125.190.18	192.168.254.129	0.135686000 8
	Seq=88 Ack=149 Win=64092 Len=0 [FIN, ACK]	80 → 49686 60	TCP	185.125.190.18	192.168.254.129	0.136945000 9
	Seq=149 Ack=89 Win=64239 Len=0 [ACK]	49686 → 80 54	TCP	192.168.254.129	185.125.190.18	0.137125000 10

(החץ שמופיע בין הפורטים מוצג אצלי הפוך כאשר ראש החץ הוא המקור וזנב החץ הוא היעד).

אסביר כעת את מה שקורה כאן:

ניתן לראות שנפתח לנו חיבור אחד, שכן השרת (בעל `port = 80`) מתקשר כל הזמן עם `port=49686` (הלקוח). (הערה: בתרגיל הזה שיניתי חזרה שה `seq, ack` יהיו יחסיים ולא במספרים האמיתיים שלהם משום שכבר פחות צריך להתמקד בהם).

שלוש השורות הראשונות- טקס ההיכרות הידוע- טקס לחיצת הידיים, `syn`, `syn ack`, `ack` קובעים על סיקוונס נאמבר של כל אחד והשני שולח לו אישור (הלקוח מתחיל עם הודעה לשרת, השרת שולח לו אישור עם הסיקוונס נאמבר שלו והלקוח שולח לו אישור).

כאן מגיע תורו של פרוטוקול HTTP עם ההודעה הבאה (שורה 4):

Frame 4: 141 bytes on wire (1128 bits), 141 bytes captured (1128 bits) <		
Ethernet II, Src: VMware_4c:43:e7 (00:0c:29:4c:43:e7), Dst: VMware_ec:04:0a (00:50:56:ec:04:0a) <		
Internet Protocol Version 4, Src: 192.168.254.129, Dst: 185.125.190.18 <		
Transmission Control Protocol, Src Port: 49686, Dst Port: 80, Seq: 1, Ack: 1, Len: 87 <		
Hypertext Transfer Protocol <		
0000	00 50 56 ec 04 0a 00 0c 29 4c 43 e7 08 00 45 00	·PV·····)LC···E·
0010	00 7f f9 80 40 00 40 06 0a 3e c0 a8 fe 81 b9 7d	·····@·@· ·>·····}
0020	be 12 c2 16 00 50 00 3d f4 89 05 3d 7a be 50 18	·····P·= ···=z·P·
0030	fa f0 85 59 00 00 47 45 54 20 2f 20 48 54 54 50	···Y··GE T / HTTP
0040	2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 63 6f 6e 6e	/1.1··Ho st: conn
0050	65 63 74 69 76 69 74 79 2d 63 68 65 63 6b 2e 75	ectivity -check.u
0060	62 75 6e 74 75 2e 63 6f 6d 0d 0a 41 63 63 65 70	buntu.co m··Accep
0070	74 3a 20 2a 2f 2a 0d 0a 43 6f 6e 6e 65 63 74 69	t: */*·· Connecti
0080	6f 6e 3a 20 63 6c 6f 73 65 0d 0a 0d 0a	on: clos e····

ניתן לראות שהיעד הוא השרת, והמקור הוא הלקוח (לפי הפורטים והIPים),

תוכן ההודעה עצמה:

```
GET / HTTP/1.1\r\n
Host: connectivity-check.ubuntu.com\r\n
Accept: */*\r\n
Connection: close\r\n
\r\n
```

"/ GET"- כאשר הבקשה ריקה ורק מקלידים localhost ומחפשים את הקובץ index.html, אותו שיניתי ולכן הוא נפתח לנו.

ו"Connection: close" בשביל לסגור את החיבור עם השרת לאחר פתיחת הקובץ, וסיום עם שתי שורות חדשות לציון סיום ההודעה כידוע לנו (על בשרינו) מהתרגיל הקודם.

בשורה הבאה זה בפרוטוקול TCP שוב להחזרת האישור על קבלת ההודעה ומיד לאחריה שוב בפרוטוקול HTTP מהשרת ללקוח בחזרה עם ההודעה הבאה:

Frame 6: 201 bytes on wire (1608 bits), 201 bytes captured (1608 bits)		
Ethernet II, Src: VMware_ec:04:0a (00:50:56:ec:04:0a), Dst: VMware_4c:43:e7 (00:0c:29:4c:43:e7)		
Internet Protocol Version 4, Src: 185.125.190.18, Dst: 192.168.254.129		
Transmission Control Protocol, Src Port: 80, Dst Port: 49686, Seq: 1, Ack: 88, Len: 147		
Hypertext Transfer Protocol		
0000	00 0c 29 4c 43 e7 00 50 56 ec 04 0a 08 00 45 00	··)LC··P V·····E·
0010	00 bb dd 7d 00 00 80 06 26 05 b9 7d be 12 c0 a8	···}··· &··}····
0020	fe 81 00 50 c2 16 05 3d 7a be 00 3d f4 e0 50 18	···P···= z··=··P·
0030	fa f0 ca 4b 00 00 48 54 54 50 2f 31 2e 31 20 32	···K··HT TP/1.1 2
0040	30 34 20 4e 6f 20 43 6f 6e 74 65 6e 74 0d 0a 73	04 No Co ntent··s
0050	65 72 76 65 72 3a 20 6e 67 69 6e 78 2f 31 2e 31	erver: n ginx/1.1
0060	34 2e 30 20 28 55 62 75 6e 74 75 29 0d 0a 64 61	4.0 (Ubu ntU)··da
0070	74 65 3a 20 54 75 65 2c 20 31 37 20 4a 61 6e 20	te: Tue, 17 Jan
0080	32 30 32 33 20 31 33 3a 31 31 3a 35 36 20 47 4d	2023 13: 11:56 GM
0090	54 0d 0a 78 2d 6e 65 74 77 6f 72 6b 6d 61 6e 61	T··x-net workmana
00a0	67 65 72 2d 73 74 61 74 75 73 3a 20 6f 6e 6c 69	ger-stat us: onli
00b0	6e 65 0d 0a 63 6f 6e 6e 65 63 74 69 6f 6e 3a 20	ne··conn ection:

```
HTTP/1.1 204 No Content\r\n
server: nginx/1.14.0 (Ubuntu)\r\n
date: Tue, 17 Jan 2023 13:11:56 GMT\r\n
x-networkmanager-status: online\r\n
connection: close\r\n
\r\n\r\n
```

(הסיום אכן קורה כראוי משום שהconnection mode בהודעות בפרוטוקול HTTP הוא אכן close).

כעת עם ifconfig נקבל מידע:

```
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.254.129 netmask 255.255.255.0 broadcast 192.168.254.255
    inet6 fe80::eaf7:62fd:b30c:4de2 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:4c:43:e7 txqueuelen 1000 (Ethernet)
    RX packets 145895 bytes 165215763 (165.2 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 52172 bytes 12131719 (12.1 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 9521 bytes 1340192 (1.3 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 9521 bytes 1340192 (1.3 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

(שם כרטיס : ens33 , IP : 192.168.254.129)

לכן נרץ,

```
sudo ethtool -K ens33 tx off sg off tso off
```

על מנת לבטל את מנגנון segmentation offload.

ועכשיו, נתחבר לדפדפן מהמחשב השני ונרשום את כתובת ה־IP 192.168.254.129 על מנת לקבל את קובץ index.html מהמחשב השני, ואכן הוא רץ לנו. נסיני (כמובן) את התעבורה בוויירשארק ונספצי (מלשון ספציפי, שוב) לקבלת:

	Info	Length	Protocol	Destination	Source	Time
...Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P [SYN]	80 → 63373 66		TCP	192.168.254.129	192.168.254.1	0.000000000 1
...Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SA [SYN, ACK]	63373 → 80 66		TCP	192.168.254.1	192.168.254.129	0.002422000 2
Seq=1 Ack=1 Win=131328 Len=0 [ACK]	80 → 63373 54		TCP	192.168.254.129	192.168.254.1	0.002842000 3
GET / HTTP/1.1 [597]			HTTP	192.168.254.129	192.168.254.1	0.003154000 4
Seq=1 Ack=544 Win=64128 Len=0 [ACK]	63373 → 80 60		TCP	192.168.254.1	192.168.254.129	0.003735000 5
HTTP/1.1 200 OK (text/html) 1514			HTTP	192.168.254.1	192.168.254.129	0.016216000 6
Continuation 1514			HTTP	192.168.254.1	192.168.254.129	0.016311000 7
Continuation 605			HTTP	192.168.254.1	192.168.254.129	0.016367000 8
Seq=544 Ack=3472 Win=131328 Len=0 [ACK]	80 → 63373 54		TCP	192.168.254.129	192.168.254.1	0.018898000 9
...Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P [SYN]	80 → 63372 66		TCP	192.168.254.129	192.168.254.1	0.998849000 10
...Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SA [SYN, ACK]	63372 → 80 66		TCP	192.168.254.1	192.168.254.129	0.999955000 11
Seq=1 Ack=1 Win=131328 Len=0 [ACK]	80 → 63372 54		TCP	192.168.254.129	192.168.254.1	1.002814000 12
Seq=3472 Ack=544 Win=64128 Len=0 [FIN, ACK]	63373 → 80 60		TCP	192.168.254.1	192.168.254.129	5.025425000 13
Seq=544 Ack=3473 Win=131328 Len=0 [ACK]	80 → 63373 54		TCP	192.168.254.129	192.168.254.1	5.026459000 14

IP לקוח (דפדפן המבקש) 192.168.254.1, IP שרת (המחשב עם index.html) 192.168.254.129, כמוזכר לעיל, port לקוח : 63373, port שרת : 80, שוב. port לקוח : 63373

שוב. שלוש השורות הראשונות לטקס ההיכרות הידוע.

שורה ארבע, פרוטוקול HTTP עם תוכן הבקשה מהדפדפן-

Frame 4: 597 bytes on wire (4776 bits), 597 bytes captured (4776 bits) on Ethernet II, Src: VMware\_c0:00:08 (00:50:56:c0:00:08), Dst: VMware\_4c:43:e7 (00:0c:29:4c:43:e7)

Internet Protocol Version 4, Src: 192.168.254.1, Dst: 192.168.254.129

Transmission Control Protocol, Src Port: 63373, Dst Port: 80, Seq: 1, Ack: 1, Len: 543

Hypertext Transfer Protocol

0000	00 0c 29 4c 43 e7 00 50 56 c0 00 08 08 00 45 00	..)LC.P V.....E
0010	02 47 1c 7c 40 00 80 06 5e 60 c0 a8 fe 01 c0 a8	.G @...^.....
0020	fe 81 f7 8d 00 50 f6 f2 ee 4d bc b0 20 10 50 18	....P...M...P.
0030	02 01 0e 00 00 00 47 45 54 20 2f 20 48 54 54 50	.....GE T / HTTP
0040	2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 31 39 32 2e	/1.1..Host: 192.
0050	31 36 38 2e 32 35 34 2e 31 32 39 0d 0a 43 6f 6e	168.254. 129..Con
0060	6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c	nection: keep-al
0070	69 76 65 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73	ive-Upgrade:Ins
0080	65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20	ecure-Requests:
0090	31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d	1..User-Agent: M
00a0	6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64	ozilla/5.0 (Wind
00b0	6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e	ows NT 1 0.0; Win

## כאשר התוכן עצמו-

```
GET / HTTP/1.1\r\n
Host: 192.168.254.129\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/109.0.0.0 Safari/537.36\r\n
ext/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: he-IL,he;q=0.9,en-US;q=0.8,en;q=0.7\r\n
If-None-Match: "29bd-5f2750b4e939f-gzip"\r\n
If-Modified-Since: Tue, 17 Jan 2023 12:43:18 GMT\r\n
\r\n
```

שוב- / get לבקשה עם 'path= 'index.html', והפעם ה-connection mode keep alive, (ושוב בסיום ההודעה שתי שורות חדשות ריקות).

חבילה הבאה (5) עם אישור ACK מהשרת ללקוח, ובתגובה השרת שולח ללקוח שלוש חבילות (בהמשכים) עם תוכן התשובה בפרוטוקול HTTP-

ההתחלה, המופיעה בחבילה הראשונה מבין השלוש, אותה אנחנו עוד יכולים להבין-

```
HTTP/1.1 200 OK\r\n
Date: Tue, 17 Jan 2023 14:18:48 GMT\r\n
Server: Apache/2.4.52 (Ubuntu)\r\n
Last-Modified: Tue, 17 Jan 2023 12:43:18 GMT\r\n
ETag: "29bd-5f2750b4e939f-gzip"\r\n
Accept-Ranges: bytes\r\n
Vary: Accept-Encoding\r\n
Content-Encoding: gzip\r\n
Content-Length: 3132\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html\r\n
\r\n
```

התוכן פותח באישור לבקשה עם "OK", connection: Keep-Alive עם timeout=5 Keep-Alive (עליו נדבר בהמשך) Content-Length: 3132, שזה אורך הקובץ.

ושאר התוכן הוא הביטים של הקובץ index.html אותו שולחים לדפדפן שיציג.

נספרתי את אורך הטקסט שהוא לא ביטים של הקובץ שנשלח בכל חבילה, בראשון יש 393, בשני 54, ובשלישי 54, סה"כ 501 בתים שנשלחו שהם לא הקובץ מקודד, וניתן לראות שאכן סכום האורכים של החבילות (3633) פחות סכום הטקסט שהוא לא הקובץ (501) שווה ל- content length המופיע בהתחלה (3132), כידוע מהתרגיל הקודם, שמה שמופיע content length זה אורך הקובץ המקודד.

כאן יש לנו אישור מהלקוח לשרת שהוא קיבל, ונפתח לנו חיבור נוסף עם השרת, עם טקס ההיכרות.

בשורה 13 ניתן לראות שהשרת שולח בקשה לסיום החיבור, ונסתכל על הזמן ונראה שזה קורה ב-5.025, כחמש שניות אחרי שליחת החבילה הראשונה מהשרת של ה-HTTP עם timeout=5 Keep-alive כפי שראינו קודם, ואכן אחרי 5 שניות השרת מבקש לסגור את החיבור עם FIN המעיד שאין לו עוד מה לשלוח אך הוא עדיין מקשיב (הלוקוח רק שולח אישור על קבלת ההודעה אך החיבור עדיין לא נסגר).



## נריץ מגלישה בסתר לקבלת :

...Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P [SYN] 80 → 63583 66	TCP	192.168.254.129	192.168.254.1	0.951045 9
...Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SA [SYN, ACK] 63583 → 80 66	TCP	192.168.254.1	192.168.254.129	0.953086 10
Seq=1 Ack=1 Win=131328 Len=0 [ACK] 80 → 63583 54	TCP	192.168.254.129	192.168.254.1	0.953201 11
GET / HTTP/1.1 484	HTTP	192.168.254.129	192.168.254.1	0.953537 12
Seq=1 Ack=431 Win=64128 Len=0 [ACK] 63583 → 80 60	TCP	192.168.254.1	192.168.254.129	0.954167 13
HTTP/1.1 200 OK (text/html) 1514	HTTP	192.168.254.1	192.168.254.129	0.969029 14
Continuation 1514	HTTP	192.168.254.1	192.168.254.129	0.969347 15
Seq=431 Ack=2921 Win=131328 Len=0 [ACK] 80 → 63583 54	TCP	192.168.254.129	192.168.254.1	0.969410 16
Continuation 605	HTTP	192.168.254.1	192.168.254.129	0.969611 17
Seq=431 Ack=3472 Win=130816 Len=0 [ACK] 80 → 63583 54	TCP	192.168.254.129	192.168.254.1	1.017965 18
GET /icons/ubuntu-logo.png HTTP/1.1 438	HTTP	192.168.254.129	192.168.254.1	1.076148 19
Seq=3472 Ack=815 Win=64128 Len=0 [ACK] 63583 → 80 60	TCP	192.168.254.1	192.168.254.129	1.086480 20
HTTP/1.1 200 OK (PNG)[Malformed Packet] 1514	HTTP	192.168.254.1	192.168.254.129	1.097951 21
Continuation 1514	HTTP	192.168.254.1	192.168.254.129	1.098197 22
Seq=815 Ack=6392 Win=131328 Len=0 [ACK] 80 → 63583 54	TCP	192.168.254.129	192.168.254.1	1.098314 23
Continuation 741	HTTP	192.168.254.1	192.168.254.129	1.105611 24
Seq=815 Ack=7079 Win=130560 Len=0 [ACK] 80 → 63583 54	TCP	192.168.254.129	192.168.254.1	1.160383 25
Seq=7079 Ack=815 Win=64128 Len=0 [FIN, ACK] 63583 → 80 60	TCP	192.168.254.1	192.168.254.129	6.162556 30
Seq=815 Ack=7080 Win=130560 Len=0 [ACK] 80 → 63583 54	TCP	192.168.254.129	192.168.254.1	6.162662 31

IP לקוח (דפדפן המבקש) 192.168.254.1, IP שרת (המחשב עם index.html), 192.168.254.129, כמוזכר לעיל, port לקוח : 63373, port שרת : 80, שוב. ו port לקוח : 63583)

## בשורה הרביעית החבילה המוכרת לנו :

```

^ts), 484 bytes captured (3872 bits) on interface \Device\NPF_{D049580F-EF42-4A3F-A0A3-57D77949C4AF}, id 0
Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: VMware_4c:43:e7 (00:0c:29:4c:43:e7)
Internet Protocol Version 4, Src: 192.168.254.1, Dst: 192.168.254.129
Transmission Control Protocol, Src Port: 63583, Dst Port: 80, Seq: 1, Ack: 1, Len: 430
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
Host: 192.168.254.129\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
Windows NT 10.0; Win64; x64 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36\r\n
+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Accept-Encoding: gzip, deflate\r\n
Accept-Language: he-IL,he;q=0.9\r\n
\r\n
0000 00 0c 29 4c 43 e7 00 50 56 c0 00 08 00 00 45 00 --)LC p .....E-
0010 01 d6 1c 92 40 00 00 06 5e bb c0 a8 fe 01 c0 a8 -- @ .....
0020 fe 81 f8 5f 00 50 64 83 c8 f1 ee 2d 42 43 50 18 -- _Pd .....BCP-
0030 02 01 64 94 00 00 47 45 54 20 2f 20 48 54 54 50 --d---GE T / HTTP
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 31 39 32 2e /1.1--Ho st: 192.
0050 31 36 38 2e 32 35 34 2e 31 32 39 0d 0a 43 6f 6e 168.254. 129--Con

```

עם connection: keep-alive כמו בהרצה הקודמת.

חבילה לאחר מכן עם אישור על קבלת הבקשה, ומיד לאחר מכן רצף של שלוש חבילות עם תוכן הקובץ (רק הפעם עם עוד אישור קבלה באמצע, בשורה 18, לא באמת משנה לפעמים זה ככה ולפעמים ככה)

והפעם אראה שוב את תוכן החבילה הראשונה לפני הקובץ המקודד-

```

HTTP/1.1 200 OK\r\n
Date: Tue, 17 Jan 2023 15:02:07 GMT\r\n
Server: Apache/2.4.52 (Ubuntu)\r\n
Last-Modified: Tue, 17 Jan 2023 12:43:18 GMT\r\n
ETag: "29bd-5f2750b4e939f-gzip"\r\n
Accept-Ranges: bytes\r\n
Vary: Accept-Encoding\r\n
Content-Encoding: gzip\r\n
Content-Length: 3132\r\n
Keep-Alive: timeout=5, max=100\r\n
Connection: Keep-Alive\r\n
Content-Type: text/html\r\n
\r\n

```

שזה כמו קודם, ולאחר שהלקוח מקבל את הקובץ index.html הדפדפן שולח עוד בקשה בשורה 19:

```
ts), 438 bytes captured (3504 bits) on interface \Device\NPF_{D049580F-EF42-4A3F-A0A3-57D77949C4AF}, id 0
Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: VMware_4c:43:e7 (00:0c:29:4c:43:e7)
Internet Protocol Version 4, Src: 192.168.254.1, Dst: 192.168.254.129
Transmission Control Protocol, Src Port: 63583, Dst Port: 80, Seq: 431, Ack: 3472, Len: 384
Hypertext Transfer Protocol
GET /icons/ubuntu-logo.png HTTP/1.1\r\n
Host: 192.168.254.129\r\n
Connection: keep-alive\r\n
Windows NT 10.0; Win64; x64; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.0.0 Safari/537.36\r\n
0000 00 0c 29 4c 43 e7 00 50 56 c0 00 08 08 00 45 00 ..)LC .P V.....E-
0010 01 a8 1c 95 40 00 80 06 5e e6 c0 a8 fe 01 c0 a8 ...@...^.....
0020 fe 81 f8 5f 00 50 64 83 ca 9f ee 2d 4f d2 50 18 ..._Pd:....O.P-
0030 01 ff 8d 1a 00 00 47 45 54 20 2f 69 63 6f 6e 73 .....GE T /icons
0040 2f 75 62 75 6e 74 75 2d 6c 6f 67 6f 2e 70 6e 67 /ubuntu- logo.png
0050 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a HTTP/1.1 -Host:
0060 20 31 39 32 2e 31 36 38 2e 32 35 34 2e 31 32 39 192.168 .254.129
0070 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 --Conne ction: ke
0080 65 70 2d 61 6c 69 76 65 0d 0a 55 73 65 72 2d 41 ep-alive --User-A
0090 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e gent: Mo zilla/5.
00a0 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 0 (Windo ws NT 10
00b0 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36 34 29 20 .0; Win6 4; x64)
```

"GET /icons/ubuntu/logo.png"- מבקש את הקובץ בנתיב שליד ה-GET ניתן לנחש שזה הלוגו של אובונטו וכנראה שלאחר קריאה של index.html הדפדפן ראה במהלך הביצוע צריך את הקובץ הזה ולכן מבקש אותו מהשרת, השרת בתגובה שוב לאורך שלוש חבילות שולח את הקובץ logo.png עם התוכן הזה בחבילה הראשונה:

```
HTTP/1.1 200 OK\r\n
Date: Tue, 17 Jan 2023 15:02:07 GMT\r\n
Server: Apache/2.4.52 (Ubuntu)\r\n
Last-Modified: Fri, 30 Sep 2022 04:09:50 GMT\r\n
ETag: "cfa-5e9dd2a489f80"\r\n
Accept-Ranges: bytes\r\n
Content-Length: 3322\r\n
Keep-Alive: timeout=5, max=99\r\n
Connection: Keep-Alive\r\n
Content-Type: image/png\r\n
r\n\r\n
```

ניתן לראות שכאן content type הוא image/png של תמונה (בניגוד לקודמים שהיו html/text).

ושוב 5=keep-alive: timeout שישפיע בשורה 30 שלאחר חמש שניות השרת ישלח FIN.

ההבדל בין כאן לפעמים הקודמות, הוא שבגלל שגלשנו מגלישה בסתר, הדפדפן לא מקושר לפעמים הקודמות ולכן התמונה לא שמורה אצלו (בניגוד לדפדפן למעלה, אצלו כבר הרצתי את הבקשה קודם לכן וכבר היה לו את התמונה אז הוא לא היה צריך לבקש אותה) ולכן הוא ביקש אותה.

כל זה קרה בחיבור אחד ולאחר אישורים על קבלות נגיע לשורה 30 עליה הסברתי ובשורה 31 הלקוח מחזיר אישור על קבלת החבילה עם ה-FIN אך עדיין לא מחזיר FIN משום שהדפדפן מבחינתו connection: Keep-Alive.



**חלק ב:**

לאחר הורדת שרת DNS למחשב, ושינוי *forwarders* לשרתי *DNS* של גוגל (8.8.4.4, 8.8.8.8) ושינוי *IP* של שרת ה-*DNS* לשרת שלנו, פשוט פתחתי דפדפן חדש של פיירפוקס, והסנפתי את התעבורה.

היו הרבה חבילות, העיקריות היו בתקשורת בתעבורות *DNS*, *TCP*, *NTP* אך בתמונה כאן ובקובץ ה-*pcap* אציג רק את החבילות מסוג *DNS* וכשיהיה צורך ארחיב במילים על תעבורת *TCP*.

אז לאחר ספיצוף:

No.	Time	Source	Destination	Protocol	Length	Info
102	15.970156	192.168.254.129	8.8.8.8	DNS	107	Standard query 0xcd4f A detectportal.firefox.com OPT
103	15.971996	192.168.254.129	8.8.8.8	DNS	107	Standard query 0x4b63 AAAA detectportal.firefox.com OPT
104	15.987619	8.8.8.8	192.168.254.129	DNS	206	Standard query response 0xcd4f A detectportal.firefox.com CNAME
105	15.988408	8.8.8.8	192.168.254.129	DNS	218	Standard query response 0x4b63 AAAA detectportal.firefox.com
135	16.903226	192.168.254.129	8.8.8.8	DNS	104	Standard query 0x128c A a1887.dscq.akamai.net OPT
136	16.905896	192.168.254.129	8.8.8.8	DNS	104	Standard query 0x81e7 AAAA a1887.dscq.akamai.net OPT
137	16.969600	8.8.8.8	192.168.254.129	DNS	124	Standard query response 0x128c A a1887.dscq.akamai.net A
138	16.970536	8.8.8.8	192.168.254.129	DNS	148	Standard query response 0x81e7 AAAA a1887.dscq.akamai.net AAA
146	18.448244	192.168.254.2	192.168.254.129	DNS	100	Standard query 0x70b9 A connectivity-check.ubuntu.com OPT
149	18.464713	192.168.254.2	192.168.254.129	DNS	428	Standard query response 0x70b9 A connectivity-check.ubuntu.co
159	18.491880	192.168.254.129	8.8.8.8	DNS	140	Standard query 0xb6f6 A prod.content-signature-chains.prod.we
162	18.553695	8.8.8.8	192.168.254.129	DNS	144	Standard query response 0xb6f6 A prod.content-signature-chain
197	19.889387	192.168.254.129	8.8.8.8	DNS	126	Standard query 0x5a19 A prod.ingestion-edge.prod.dataops.mozg
198	19.906932	8.8.8.8	192.168.254.129	DNS	130	Standard query response 0x5a19 A prod.ingestion-edge.prod.dat
233	20.156757	192.168.254.129	8.8.8.8	DNS	100	Standard query 0x4cc3 A ocsip.digicert.com OPT
234	20.157642	192.168.254.129	8.8.8.8	DNS	100	Standard query 0x1d29 AAAA ocsip.digicert.com OPT
235	20.219269	8.8.8.8	192.168.254.129	DNS	136	Standard query response 0x4cc3 A ocsip.digicert.com CNAME
236	20.220055	8.8.8.8	192.168.254.129	DNS	185	Standard query response 0x1d29 AAAA ocsip.digicert.com CNAME
277	21.612166	192.168.254.129	8.8.8.8	DNS	104	Standard query 0x1032 A reddit.map.fastly.net OPT
278	21.614571	192.168.254.129	8.8.8.8	DNS	104	Standard query 0x3f5 AAAA reddit.map.fastly.net OPT
279	21.630486	8.8.8.8	192.168.254.129	DNS	156	Standard query response 0x1032 A reddit.map.fastly.net A
280	21.635559	192.168.254.129	8.8.8.8	DNS	94	Standard query 0x75e8 AAAA twitter.com OPT

בתעבורת *TCP* שקורית קודם, הדפדפן פותח קשר עם השרת (בעל ה-*IP* של המחשב שלנו) ושולח לו בקשות לכתובות של אתרים מסוימים (על החלק הזה הסברתי בחלק א לכן כאן זה בקצרה) וכאן מגיע החלק שלנו:

שרת ה-*DNS* שלנו (בעל  $ip=192.168.254.129$ ), כשל המחשב כולו) שולח לשרת של גוגל כפי שהגדרנו לו (עם  $IP=8.8.8.8$ ) ומבקש ממנו כל מיני כתובות לפי הדומיינים שלהם (כדוגמת השורה הראשונה בתמונה, חבילה 102, "detectportal.firefox.com") והשרת בתשובה מחזיר לו את כתובת ה-*IP* שלהם כפי שראינו בהרצאה.

אדגים כאן על הדו שיח הראשון:

בקשת השרת המקומי:

Packet 102 - VMware Network Adapter VMnet8	Wireshark - Packet 103 - VMware Network Adapter VMnet8
Interface \Device\NPF_{D049580F-EF42-4A3F-A0A3-57D77949C4AF}, id 0 <	Interface \Device\NPF_{D049580F-EF42-4A3F-A0A3-57D77949C4AF}, id 0 <
Src: 192.168.254.129, Dst: VMware_ec:04:0a (00:50:56:ec:04:0a) <	Src: 192.168.254.129, Dst: VMware_ec:04:0a (00:50:56:ec:04:0a) <
Internet Protocol Version 4, Src: 192.168.254.129, Dst: 8.8.8.8 <	Internet Protocol Version 4, Src: 192.168.254.129, Dst: 8.8.8.8 <
User Datagram Protocol, Src Port: 60549, Dst Port: 53 <	User Datagram Protocol, Src Port: 50712, Dst Port: 53 <
Domain Name System (query) <	Domain Name System (query) <
Transaction ID: 0xcd4f <	Transaction ID: 0x4b63 <
Flags: 0x0110 Standard query <	Flags: 0x0110 Standard query <
Questions: 1 <	Questions: 1 <
Answer RRs: 0 <	Answer RRs: 0 <
Authority RRs: 0 <	Authority RRs: 0 <
Additional RRs: 1 <	Additional RRs: 1 <
Queries <	Queries <
detectportal.firefox.com: type A, class IN <	detectportal.firefox.com: type AAAA, class IN <
Name: detectportal.firefox.com <	Name: detectportal.firefox.com <
[Name Length: 24] <	[Name Length: 24] <
[Label Count: 3] <	[Label Count: 3] <
Type: A (Host Address) (1) <	Type: AAAA (IPv6 Address) (28) <
Class: IN (0x0001) <	Class: IN (0x0001) <
Additional records <	Additional records <

שתי החבילות הראשונות (הראשונה משמאל והשנייה מימין), ניתן לראות שבראשונה השרת מבקש *type A* ובשנייה *type AAAA* (*IPv6*), והשרת מנסה את שתי הגרסאות משום שעדיין קיימים דומיינים כאלה ודומיינים כאלה.

והשדות המוכרים לנו מההרצאה והתרגול: *Name: detectportal.firefox.com Class: IN* (כדומיין).

ותשובת השרת של גוגל (לאחר חיפוש אצלו לפי שיטת ה-*root* שראינו בהרצאה): השרת שולח לו שתי תשובות (בשתי החבילות 104-105, כאשר הראשונה עם *IPv4* השנייה עם *IPv6*, אראה



כאן את הראשונה בעלת *IPv4* - חבילה 104 :

```

Questions: 1
Answer RRs: 3
Authority RRs: 0
Additional RRs: 1
Queries
detectportal.firefox.com: type A, class IN
Name: detectportal.firefox.com
[Name Length: 24]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
Answers
detectportal.firefox.com: type CNAME, class IN, cname detectportal.prod.mozaws.net
detectportal.prod.mozaws.net: type CNAME, class IN, cname prod.detectportal.prod.cloudops.mozgcp.net
prod.detectportal.prod.cloudops.mozgcp.net: type A, class IN, addr 34.107.221.82
Additional records

```

ובאמת כידוע לנו, השרת מחזיר עם התשובה את הבקשה ב*Queries* ואז עם תשובות ב*Answers* בצורה הבאה:

כל פעם השרת מפנה אותו לכתובת הבאה אך גם בודק לו אותה עד שמגיע *ip* ובמקרה שלנו מסוג *IPv4*:

*detectportal.firefox.com* (המבוקש מהשרת) -> *detectportal.prod.mozaws.net* ->  
*prod.detectportal.prod.cloudops.mozgcp.net* = 34.107.221.82

ניתן לשער שזה איזה דומיין של הדפדפן *firefox* שצריך על מנת לפתוח אותו, מכאן הדפדפן ממשיך ונתקל בעוד דומיינים שהוא צריך ומבקש גם אותם וקורה בדומה למה שהצגתי כאן.

ניתן לראות לאחר הרצה נוספת וסינון שוב:

	Info	Length	Protocol	Destination	Source	Time	No
Standard query 0x7c81 A www.wireshark.org OPT 100			DNS	8.8.8.8	192.168.254.129	4.101801000	7
Standard query 0xfe61 AAAA www.wireshark.org OPT 100			DNS	8.8.8.8	192.168.254.129	4.102229000	8
Standard query 0xc36c AAAA youtube-ui.l.google.com OPT 106			DNS	8.8.8.8	192.168.254.129	4.105231000	9
Standard query 0x6ab6 A star-mini.c10r.facebook.com OPT 110			DNS	8.8.8.8	192.168.254.129	4.113998000	10
Standard query 0xd299 AAAA star-mini.c10r.facebook.com OPT 110			DNS	8.8.8.8	192.168.254.129	4.114251000	11
Standard query response 0x7c81 A www.wireshark.org A 104.26.1		136	DNS	192.168.254.129	8.8.8.8	4.164149000	12
Standard query response 0xfe61 AAAA www.wireshark.org AAAA 26		172	DNS	192.168.254.129	8.8.8.8	4.165427000	13
Standard query 0x32f7 AAAA dyna.wikimedia.org OPT 101			DNS	8.8.8.8	192.168.254.129	4.169539000	14
Standard query response 0xd299 AAAA star-mini.c10r.facebook.c		126	DNS	192.168.254.129	8.8.8.8	4.175443000	15
Standard query response 0x6ab6 A star-mini.c10r.facebook.com		114	DNS	192.168.254.129	8.8.8.8	4.177643000	16
Standard query 0x7ae4 A reddit.map.fastly.net OPT 104			DNS	8.8.8.8	192.168.254.129	4.180239000	17
Standard query 0xcd02 AAAA reddit.map.fastly.net OPT 104			DNS	8.8.8.8	192.168.254.129	4.180520000	18
Standard query response 0xc36c AAAA youtube-ui.l.google.com A 206			DNS	192.168.254.129	8.8.8.8	4.196677000	19
Standard query 0xf407 AAAA twitter.com OPT 94			DNS	8.8.8.8	192.168.254.129	4.199136000	20
Standard query response 0xcd02 AAAA reddit.map.fastly.net SOA 153			DNS	192.168.254.129	8.8.8.8	4.201011000	21
Standard query response 0xf407 AAAA twitter.com SOA ns1.p26.d		154	DNS	192.168.254.129	8.8.8.8	4.215558000	22
Standard query response 0x7ae4 A reddit.map.fastly.net A 151		156	DNS	192.168.254.129	8.8.8.8	4.245220000	23
Standard query response 0x32f7 AAAA dyna.wikimedia.org AAAA 2		117	DNS	192.168.254.129	8.8.8.8	4.327106000	24

ישנן הרבה פחות חבילות מתקשורת ה*DNS* וכל התקשורת שקרתה בהרצה הראשונה (בתמונה למעלה) בכלל לא קורית כאן משום שהשרת שמר *cache* ולכן הוא לא פונה לשרת של גוגל משום שהדומיינים ו*IP* שלהם שמורים אצלו.

הערה: בכל זאת הוא כן פונה ואני לא יודע בדיוק למה, אלה כתובות שהוא לא שמר ב*cache* שלו, כנראה בגלל שהוא לא היה צריך אותן בפעם הקודמת, או שהוא לא ראה לנכון לשמור אותן וראה לנכון יותר לשמור את הראשונות, חיפשתי בהרצה הראשונה והכתובות האלו לא הופיעו שם אבל אולי זה בגלל שעצרתי את ההרצה קודם, לא יודע.

הערה 2: ניתן לראות בזמנים שהתהליך כולו קורה הרבה יותר מהר משום שלדפדפן ולשרת המקומי יש פחות עבודה לבצע.

כעת נכנסתי ליוטיוב (דומיין- [www.youtube.com](http://www.youtube.com)) ולאחר הרצת הפקודה `sudo rndc dumpdb -cache` נראה את הכתובות השמורות ב- *cache* :

```
xB8DUzRfmr17nPMjgA== )
; answer
ip4only.arpa.      8368      A      192.0.0.170
                   8368      A      192.0.0.171
; answer
apis.google.com.   13277     CNAME   plus.l.google.com.
; answer
lh3.googleusercontent.com. 9962 CNAME   googlehosted.l.googleusercontent.com.
; answer
shavar.services.mozilla.com. 11767 CNAME   shavar.prod.mozaws.net.
; answer
www.youtube.com.   11985     CNAME   youtube-ui.l.google.com.
; answer
o.lencr.edgesuite.net. 16711 CNAME   a1887.dscq.akamai.net.
; glue
a.root-servers.net. 513742    A      198.41.0.4
; glue
                   513742    AAAA   2001:503:ba3e::2:30
; glue
b.root-servers.net. 513742    A      199.9.14.201
; glue
                   513742    AAAA   2001:500:200::b
; glue
```

ואכן יש כאן את הדומיין שמור.

כעת נגלוש לויקיפדיה שאכן לא מופיע ב- *cache* ונייצא שוב ואכן :

```
; glue
l.root-servers.net. 513061    A      199.7.83.42
; glue
                   513061    AAAA   2001:500:9f::42
; glue
m.root-servers.net. 513061    A      202.12.27.33
; glue
                   513061    AAAA   2001:dc3::35
; answer
example.org.        14057     A      93.184.216.34
; answer
                   14057     RRSIG   A 8 2 86400 (
20230205200535 20230115153320 43798 example.org.
YLYXRbzzw0JV/hKy/5137To7UY+fXeBFf3Ro
yJHqM/Vr6Im7lpQ5JMExx+HAmlo/sVwBa30
eH8GakILC6uoaFltDj4tKtuYawkkjlrUGaTp
ARWVgraqKNXbbiriM7e2Dd5ndTZqzkX6PP1Q
BXmVEn8lEOtwBQKKi+JFBIYEbBk= )
; answer
www.wikipedia.org.  16173     CNAME   dyna.wikimedia.org.
;
```

כעת אשנה את הדברים המבוקשים וככה נראה הקובץ שלי

```
@      IN      SOA      biu.ac.il. root.biu.ac.il. (
                        5          ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200    ; Expire
                        604800 )   ; Negative Cache TTL
;
@      IN      NS      ns.biu.ac.il.
ns     IN      A        127.0.0.1
www.biu.ac.il IN      A        192.168.254.129
@      IN      MX      10 mail.biu.ac.il
mail.biu.ac.il IN      A        192.168.254.129
@      IN      AAAA    ::1
```

כעת נבצע הרצה של *nslookup* לבקשת *ns.biu.ac.il*

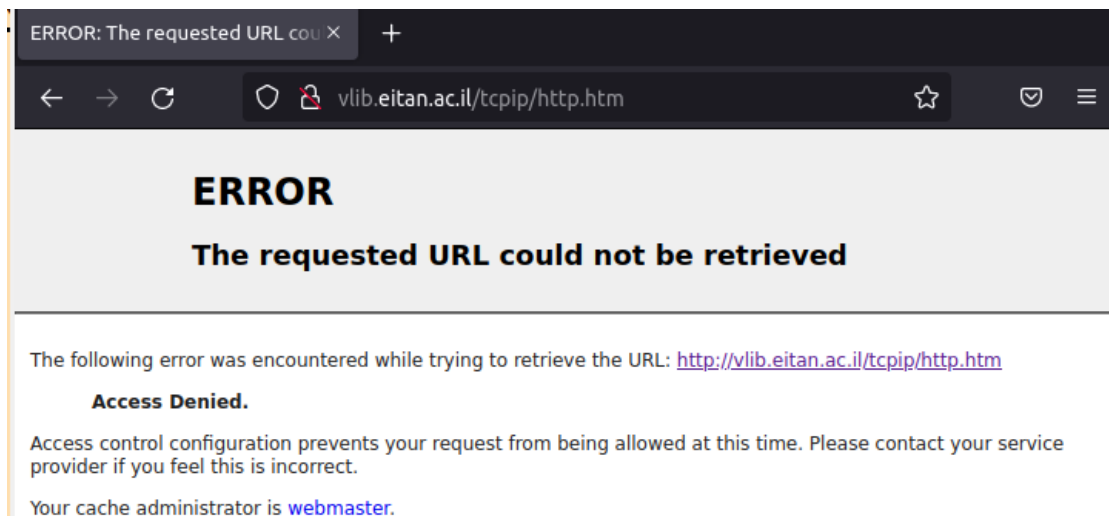
```
> ns.biu.ac.il
Server:          192.168.254.129
Address:         192.168.254.129#53

Name:   ns.biu.ac.il
Address: 127.0.0.1
```

אך כאן *wireshark* משום מה לא הסניף לי כלום (ניסיתי מלא פעמים ועכשיו אני כבר על סף ייאוש) לכן איני יכול לצרף את זה.

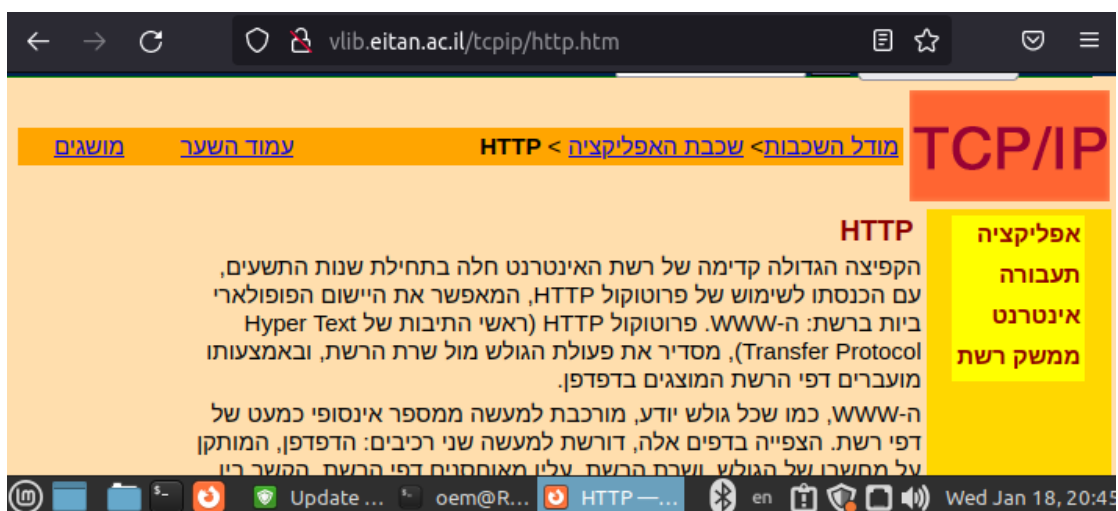
חלק ג:

לאחר התקנת שרת proxy נתחבר לכתובת <http://vlib.eitan.ac.il/tcpip/http.htm> ואכן:



*Access denied*

לאחר השינויים המבוקשים (*http\_access allow all*) אכן עובד:



כעת גלשתי לאתר [http://help.websiteos.com/websites/example\\_of\\_a\\_simple\\_html\\_page.htm](http://help.websiteos.com/websites/example_of_a_simple_html_page.htm) משום שלאחר הקודם כבר גלשתי וכשהסנפתי זה לא הראה את כל הדברים שקורים, לכן גלשתי אליו והסנפתי:

	Info	Length	Protocol	Destination	Source	Time
1	http://help.websiteos.com/websites/whtopic.js	HTTP/1.1 477	HTTP	192.168.254.129	192.168.254.1	1.849829 152
		HTTP/1.1 200 OK 897	HTTP	192.168.254.129	216.251.32.98	1.992663 162
		HTTP/1.1 200 OK 428	HTTP	192.168.254.1	192.168.254.129	1.998596 164
		Continuation 599	HTTP	192.168.254.1	192.168.254.129	1.998794 165
		Continuation 60	HTTP	192.168.254.1	192.168.254.129	1.999226 167
	GET /websites/whmsg.js	HTTP/1.1 537	HTTP	216.251.32.98	192.168.254.129	2.037604 185
	GET /websites/whver.js	HTTP/1.1 537	HTTP	216.251.32.98	192.168.254.129	2.037814 187
	GET /websites/whproxy.js	HTTP/1.1 539	HTTP	216.251.32.98	192.168.254.129	2.038183 189
	GET /websites/whtopic.js	HTTP/1.1 539	HTTP	216.251.32.98	192.168.254.129	2.046113 193
	GET /websites/whutils.js	HTTP/1.1 539	HTTP	216.251.32.98	192.168.254.129	2.047878 195
		HTTP/1.1 200 OK 1101	HTTP	192.168.254.129	216.251.32.98	2.209261 215
		HTTP/1.1 200 OK 838	HTTP	192.168.254.129	216.251.32.98	2.210322 216
		HTTP/1.1 200 OK 1514	HTTP	192.168.254.129	216.251.32.98	2.212631 217
		Continuation 1514	HTTP	192.168.254.129	216.251.32.98	2.213532 220
		Continuation 1248	HTTP	192.168.254.129	216.251.32.98	2.213579 221
		HTTP/1.1 200 OK 471	HTTP	192.168.254.1	192.168.254.129	2.214227 224
		HTTP/1.1 200 OK 471	HTTP	192.168.254.1	192.168.254.129	2.214342 225
		Continuation 772	HTTP	192.168.254.1	192.168.254.129	2.214705 226
		Continuation 509	HTTP	192.168.254.1	192.168.254.129	2.214842 228
		HTTP/1.1 200 OK 472	HTTP	192.168.254.1	192.168.254.129	2.214951 230
		Continuation 60	HTTP	192.168.254.1	192.168.254.129	2.215076 231
		Continuation 60	HTTP	192.168.254.1	192.168.254.129	2.215167 232
		Continuation 1514	HTTP	192.168.254.1	192.168.254.129	2.215252 233
		Continuation 1514	HTTP	192.168.254.1	192.168.254.129	2.215294 235

(*IP*) של המחשב עם השרת פרוקסי הוא 192.168.254.129 ו(*IP*) של המחשב השני המבקש הוא (192.168.254.1)

אכן ניתן לראות ראשית שכל בקשה לא קורית בחיבור אחד אלא בשניים למשל כאן:

בשורות 215-221 זה השרת אליו פונה השרת שלנו שולח לשרת עם הפרוקסי, והשרת עם הפרוקסי שולח למחשב עם הדפדפן בשורות 224-228 וניתן לראות שזה קורה בשני חיבורים שונים.

בנוסף נראה כי אכן השרת שולח לדפדפן את הקובץ כולו (לאחר שהוא מוריד אותו אליו מהחיבור שקיבל ממנו) לדוגמה בחבילה 226 (*continuation*) מבין חבילות 224-228:

Frame 57: 772 bytes on wire (6176 bits), 772 bytes captured (6176 bits) <  
 Ethernet II, Src: VMware\_4c:43:e7 (00:0c:29:4c:43:e7), Dst: VMware\_c0:00:08 (00:50:56:c0:00:08) <  
 Internet Protocol Version 4, Src: 192.168.254.129, Dst: 192.168.254.1 <  
 Transmission Control Protocol, Src Port: 3128, Dst Port: 60506, Seq: 418, Ack: 422, Len: 718 <  
 Hypertext Transfer Protocol <  
 File Data: 718 bytes <  
 Data (718 bytes) <  
 ...Data: 3243370d0a1f8b080000000000000000394555d6fda30147d4e7e85cb0324ea16022d61d264  
 [Length: 718]

```

^ 0000 00 50 56 c0 00 08 00 0c 29 4c 43 e7 08 00 45 00 ..PV....)LC...E.
0010 02 f6 78 74 40 00 40 06 41 b9 c0 a8 fe 81 c0 a8 ..xt@.A.....
0020 fe 01 0c 38 ec 5a 51 36 49 a0 62 cd d8 d4 50 18 ...8-ZQ6 I.b..P.
0030 01 f5 73 39 00 00 32 43 37 0d 0a 1f 8b 08 00 00 ...s9..2C 7.....
0040 00 00 00 00 03 94 55 5d 6f da 30 14 7d 4e 7e 85 .....U] o-0.}N~
0050 cb 03 24 ea 16 02 2d 61 d2 64 a4 69 ea 34 b4 d1 ..$...-a .d-i-4..
0060 4e aa b4 3e 9b cc 30 af c4 ce ec 00 dd 56 fe db N->...0- ....V..
0070 1c 7f 24 26 66 a2 7b 00 89 7b cf b9 dc 73 7c af ..$&f-{-{...s|.
0080 3d 1c 06 0f 78 f9 11 6f 4a 30 49 46 69 92 a6 59 =...x-o J0IFi..Y
0090 b8 43 1c ac 97 b7 68 07 57 68 23 f0 db 36 90 f9 .C...h- Wh#...6..
v 00a0 91 91 17 9a 7a 91 eb e3 c8 fc c6 0b 74 7f 4f bc ...z... ..t.O.

```

נשלחת דאטה בבתים של הקובץ עצמו ואכן זה הקובץ כולו מקודד שהשרת מעביר הלאה.

ובנוסף, אכן הDNS מתבצע משרת *proxyn* כפי שניתן לראות כל התקשורת עוברת דרכו.



הערה לבדוק: הרבה דברים קרו לבסוף לאחר הרבה ניסיונות שלא הבנתי למה הם שגו לי, על אף שאני יודע את החומר, אך המחשב שלי משום מה לפעמים מריץ דברים אחרת ואילו במחשבים אחרים זה עבד לי בניסיונות שלי. אני לא יודע אם קבצי הpcap מהwireshark וצילומים שלהם יהיו מדויקים בעקבות כך אך ניתן לראות אכן שהשקעתי בתרגיל הזה רבות ובאמת התאמצתי הרבה והשקעתי בו. אשמח להתחשבותך בנושא. תודה רבה מראש ובשעה טובה חסל סדר תרגיל.