





CERT.hr

Sadržaj

1	UVO	D3	ì
2	INST	ALACIJA I KORIŠTENJE4	•
	2.1	INSTALACIJA	1
	2.2	KORIŠTENJE	
	2.2.1	Filtriranje paketa	
	2.2.2	Analiza DNS prometa	ĵ
	2.2.3	Analiza HTTP prometa	i
3	ZAKI	LJUČAK	,

Dokument je izradio Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Ovaj dokument je vlasništvo Nacionalnog CERT–a. Namijenjen je za javnu objavu, njime se može svatko koristiti, na njega se pozivati, ali samo u izvornom obliku, bez ikakvih izmjena, uz obvezno navođenje izvora podataka. Zabranjena je bilo kakva distribucija dokumenta u elektroničkom (web stranice i dr.) ili papirnatom obliku. Korištenje ovog dokumenta protivno gornjim navodima, povreda je autorskih prava CARNet–a, a sve sukladno zakonskim odredbama Republike Hrvatske.



1 Uvod

Računala se svakim danom sve više koriste za komunikaciju. Ta komunikacija se odvija preko računalnih mreža korištenjem brojnih mrežnih protokola. Zato je važno imati mogućnost pregleda i analize mrežnog prometa.

Wireshark je najpoznatiji alat za snimanje i analizu mrežnog prometa. On omogućava snimanje mrežnog prometa odabranog mrežnog sučelja te njegovo interaktivno pregledavanje i analizu. Wireshark prepoznaje više stotina protokola te ih u svom sučelju prikazuje u strukturiranom i čitljivom formatu. Prva inačica alata nastala je 1998. godine pod imenom Ethereal, no 2006. godine projekt mijenja ime u Wireshark. Wireshark je slobodan softver (eng. *free and open source*) te je dostupan na većem broju platformi, uključujući Microsoft Windows, Linux, macOS, Solaris i BSD.

Analiza mrežnog prometa vrlo je važna u radu IT stručnjaka. Neke od važnih primjena su:

- Pomoć pri razvoju mrežnih protokola
- Traženje pogrešaka u implementaciji mrežnih protokola
- Analiziranje ponašanja zloćudnih programa

Wireshark je također odličan alat za edukaciju i upoznavanje s osnovama rada računalnih mreža i protokola.

Kao i gotovo svi drugi alati, Wireshark je moguće koristiti i u zlonamjerne svrhe. U određenim situacijama, napadač pomoću Wireshark-a može prisluškivati mrežni promet žrtve te saznati njene povjerljive podatke ako promet nije šifriran. Najveći rizik od ovakvog prisluškivanja imaju bežične (npr. Wi-Fi) mreže.

U ovom dokumentu bit će prikazan postupak instalacije alata Wireshark te jednostavni primjeri njegovog korištenja – osnovno filtriranje paketa te analiza DNS i HTTP prometa.

2 Instalacija i korištenje

2.1 Instalacija

Postupak instalacije alata Wireshark bit će opisan za operacijski sustav Windows. Koraci za instalaciju su sljedeći:

1. Prvo je potrebno preuzeti odgovarajuću inačicu Wireshark-a s <u>ove poveznice</u>. U ovom primjeru to je "Windows Installer (64-bit)".



Slika 1



2. Nakon preuzimanja i pokretanja datoteke otvara se instalacijski prozor na engleskom jeziku. Potrebno je kliknuti na *Next* za sljedeći korak.





3. U sljedećem koraku potrebno je složiti se s uvjetima korištenja klikom na *I agree*.

📕 Wireshark 2.4.3 64-bit Setup —	\times
License Agreement Please review the license terms before installing Wireshark 2.4.3 64-bit.	
Press Page Down to see the rest of the agreement.	
This text consists of three parts:	^
Part I: Some remarks regarding the license given in Part II: The actual license that covers Wireshark. Part III: Other applicable licenses. When in doubt: Part II/III is the legally binding part, Part I is just there to make it easier for people that are not familiar with the GPLv2.	1
	~
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Wireshark 2.4.3 64-bit.	
< Back I Agree Cano	cel

Slika 3



4. Potrebno je odabrati komponente koje će se instalirati kao što je prikazano na slici te kliknuti *Next*.

📕 Wireshark 2.4.3 64-bit Setup		_		×
Choose Components Choose which features of Wires	shark 2.4.3 64-bit you want to install.			
The following components are a	available for installation.			
Select components to install:	Wireshark Vireshark Wireshark 1 Wireshark 1 Vireshark 1 Or ♥ Plugins & Extensions Or ♥ User's Guide			
Space required: 172.5MB	Description Position your mouse over a compon- description.	ent to see	e its	
Wireshark Installer (tm) ———				
	< Back Ne	xt >	Ca	ncel

Slika 4

5. Zatim je potrebno odabrati gdje će u sustavu biti stvorene poveznice na Wireshark te kliknuti *Next* za sljedeći korak.

Wireshark 2.4.3 64-bit Setup	—		×
Select Additional Tasks			
Which additional tasks should be done?			
Create Shortcuts			
Wireshark Start Menu Item			
Wireshark Desktop Icon			
Wireshark Quick Launch Icon			
Wireshark Legacy Start Menu Item			
Wireshark Legacy Desktop Icon			
Wireshark Legacy Quick Launch Icon			
File Extensions			
Associate trace file extensions to Wireshark			
Associate trace file extensions to Wireshark Legacy			
○ None			
Extensions: 5vw, acp, apc, atc, bfr, cap, enc, erf, fdc, ipfix, mplog pcapng, pklg, pkt, rf5, snoop, syc, tpc, tr1, trace, trc, vwr, wpc, v	g, out, po wpz	ap,	
Wireshark Installer (tm)			
< Back Ne	xt >	Ca	incel

Slika 5



6. U ovom koraku moguće je odabrati direktorij za instalaciju alata. Nakon odabira potrebno je kliknuti *Next*.

🚄 Wireshark 2.4.3 64-bit Setup	-		\times
Choose Install Location Choose the folder in which to install Wireshark 2.4.3 64-bit.			
Choose a directory in which to install Wireshark.			
Destination Folder			
C:\Program Files\Wireshark	Bro	wse	
Space required: 172.5MB Space available: 132.0GB			
Wireshark Installer (tm)			
< Back	vext >	Car	ncel

Slika 6

7. Kako bi Wireshark mogao snimati mrežne podatke na operacijskom sustavu Windows, potrebno je instalirati program WinPcap. Klikom na *Next* prelazi se na sljedeći korak.

📕 Wireshark 2.4.3 64-bit Setup		_		×
Install WinPcap? WinPcap is required to capture live network data. Si	hould WinPca	be installed?		
Currently installed WinPcap version WinPcap is currently not installed				
Install Install Install WinPcap 4.1.3 (Use Add/Remove Programs first to uninstall a	any undetecte	ed old WinPcap	versions	5)
What is WinPcap?				
Wireshark Installer (tm)	< Back	Nexts	6	ocel
	< DOLK	Next >	Car	icei

Slika 7



8. U ovom koraku može se odabrati i instalacija alata USBPcap za snimanje USB prometa. U ovim primjerima on neće biti potreban, pa nije označen. Klikom na *Install* pokreće se instalacijski prozor potrebnog programa WinPcap.

🧲 Wireshark 2.4.3 64-bit Setup —		×
Install USBPcap?		
USBPcap is required to capture USB traffic. Should USBPcap be installed (experimental)?		
Currently installed USBPcap version		
USBPcap is currently not installed		
Instal		
Install USBPcap 1.2.0.3		
(Use Add/Remove Programs first to uninstall any undetected old USBPca	p version	s)
Important notice		
In case of issue after installation, please use the system restore point creat https://github.com/desowin/usbpcap/issues/3	ted or rea	d
What is USBPcap?		
Wireshark Installer (tm)		
< Back Install	Car	ncel

Slika 8

9. Zatim je potrebno stisnuti *Next* kako bi se prešlo na sljedeći korak.



Slika 9



10. U sljedećem koraku potrebno je složiti se s uvjetima korištenja klikom na *I agree*.



Slika 10

11. Klikom na *Install* počinje instalacija programa WinPcap.



Slika 11



12. Nakon završetka instalacije potrebno je kliknuti na *Finish* kako bi se zatvorio prozor instalacije WinPcap-a i nastavila instalacija Wireshark-a.



Slika 12

13. Nakon što je gotova instalacija Wireshark-a potrebno je kliknuti na *Next* te zatim *Finish*.

🚄 Wireshark 2.4.3 64-bit Setup		_		\times
Installation Complete Setup was completed successfully.				
Completed				
Extract: reordercap.exe Output folder: C:\Program Files\Wireshark Extract: capinfos.exe Extract: capinfos.html Output folder: C:\Program Files\Wireshark Extract: rawshark.exe Extract: rawshark.html Output folder: C:\Program Files\Wireshark Extract: user-guide.chm Completed				~
Wireshark Installer (tm)				
	< Back	Next >	Ca	ncel

Slika 13



2.2 Korištenje

Pokretanjem Wireshark-a pojavljuje se popis mrežnih sučelja računala. U ovom primjeru računalo koristi bežičnu vezu, pa će se dvoklikom na *WiFi* pokrenuti snimanje mrežnog prometa. Početni prozor Wireshark-a prikazan je na slici 14.

📕 The Wire	shark Network Analyzer -	-		×
File Edit	View Go Capture Analyze Statistics Telephony Wireless Tools Help			
	، الله الله الله الله الله الله الله الل			
📕 Apply a dis	lay filter <ctrl-></ctrl->	🔰 Ex	pression	. +
	Welcome to Wireshark			
	Capture			
	using this filter: 📕 Enter a capture filter 🔹 All interfaces shown	•		
	Ethernet			
	WiFi M Rhusteath Natural Connection			
	Bruetooth Network Connection			
	Learn			
	User's Guide · Wiki · Questions and Answers · Mailing Lists			
	You are running Wireshark 2.4.3 (v2.4.3-0-g368ba1ee37). You receive automatic updates.			
🖉 🛛 Ready to	load or capture No Packets	Pr	ofile: Def	ault 🔡

Slika 14 - Početni prozor alata Wireshark



Nakon toga otvara se glavni prozor alata te počinje snimanje paketa na odabranom mrežnom sučelju, kako je prikazano na slici 15. Osnovni elementi sučelja su (od vrha prema dnu) glavni izbornik, alatna traka s često korištenim radnjama, alatna traka za filtriranje, popis paketa, detalji odabranog paketa te prikaz bajtova odabranog paketa. U popis paketa dodaju se paketi kako dolaze odnosno odlaze s mrežnog sučelja.

Eile E Apply No.	Image: Contract of the second secon	Capture Analyze Statistics	Telephony <u>W</u> ireless <u>Too</u>	ols <u>H</u> elp				
Apply No.	Image: Constraint of the second sec	🕅 🙆 🍳 🖛 🗭 🖉 🕋 Ctrl-/>	👱 📃 📃 Q, Q, Q, I					
No.	/ a display filter <c Time 1 0.000000</c 	Ctrl-/>						
No.	Time 1 0.000000	C				🔁 🔹 Ex	pression	+
	1 0.000000	Source	Destination	Protocol	Length Info			^
		188.252.148.15	192.168.0.25	UDP	60 16666	→ 64550	Len=13	
	2 0.000120	192.168.0.25	188.252.148.15	UDP	57 64550	→ 16666	Len=15	
	3 0.608726	192.168.0.25	188.252.148.15	UDP	55 64550	→ 16666	Len=13	
	4 0.628163	188.252.148.15	192.168.0.25	UDP	60 16666	→ 64550	Len=13	
	5 1.010438	188.252.148.15	192.168.0.25	UDP	60 16666	→ 64550	Len=13	
	6 1.010559	192.168.0.25	188.252.148.15	UDP	57 64550	→ 16666	Len=15	
	7 1.611177	192.168.0.25	188.252.148.15	UDP	55 64550	→ 16666	Len=13	
	8 1.630421	188.252.148.15	192.168.0.25	UDP	60 16666	→ 64550	Len=13	
	9 1.998663	188.252.148.15	192.168.0.25	UDP	60 16666	→ 64550	Len=13	~
> EtH > Int > Use > Dat	ernet II, Src ternet Protoco er Datagram Pr ta (13 bytes)	: Technico_75:6d:af (b l Version 4, Src: 188. otocol, Src Port: 1666	of 08 00 45 00	t: IntelCor 168.0.25	E	08:d4:0c:	d7:cf:7	'6)
0000	08 04 0C 07 00 29 00 00	A A A 36 11 32 f7 bc	$f = 08 \ 00 \ 45 \ 00 \$	vum @ 6 2	.E.			
0020	00 19 41 1a	fc 26 00 15 8d 9a 94	05 0a d9 12 6dA		m			
0030	69 63 9a 6e	84 fc e9 00 00 00 00	00 ic.	n				
0.7					Disclored, 100 /	100.00/)	afila Defe	

Slika 15 - Glavni prozor alata Wireshark



Klikom na željeni paket, pod pretpostavkom da ga Wireshark razumije, njegov sadržaj prikazuje se u strukturiranom obliku. Na slici 16 prikazan je ARP (engl. *Address Resolution Protocol*) paket te je moguće vidjeti dijelove paketa uz nazive polja.

<u> </u>	WiFi						-		\times
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew <u>G</u> o <u>C</u> apt	ture <u>A</u> nalyze <u>S</u> tatistics T	elephon <u>y W</u> ireless <u>T</u> oo	ls <u>H</u> elp				
		0 I T X	ି । 🤇 🔶 🔿 🖉 🖉	📜 📃 Q, Q, Q, 🏢					
Ар	ply a di	splay filter <ctrl- :<="" td=""><td>></td><td></td><td></td><td></td><td></td><td>Expression</td><td> +</td></ctrl->	>					Expression	+
No.		Time	Source	Destination	Protocol	Length Info			^
	1564	290.279291	192.168.0.25	188.252.148.15	UDP	57 64550 → 16666 Len=15			
	1565	290.425422	192.168.0.25	146.66.152.11	UDP	126 65137 → 27018 Len=84			
	1566	290,906870	192.168.0.25	188.252.148.15	UDP	55 64550 → 16666 Len=13			
	1567	290,923187	188,252,148,15	192.168.0.25	UDP	60 16666 → 64550 Len=13			
	1568	291.279441	188.252.148.15	192.168.0.25	UDP	60 16666 → 64550 Len=13			
	1569	291,279548	192.168.0.25	188,252,148,15	UDP	57 64550 → 16666 Len=15			
	1570	291.478018	IntelCor d7:cf:76	Technico 75:6d:af	ARP	42 Who has 192.168.0.1? Tell 192.168.0.25			
	1571	291,478953	Technico 75:6d:af	IntelCor d7:cf:76	ARP	42 192.168.0.1 is at b0:c2:87:75:6d:af			
	1572	291.909802	192.168.0.25	188.252.148.15	UDP	55 64550 → 16666 Len=13			
	1577	201 022000	100 151 140 15	100 160 0 05	ЦОО	60 16666 . 64550 Lon 17			~
ΥA	ddres	s Resolution	Protocol (reply)						^
	Har	dware type: E	thernet (1)						
	Pro	tocol type: I	Pv4 (0x0800)						- 10
	Har	dware size: 6							
	Pro	tocol size: 4							
	0pc	ode: reply (2)						
	Sen	der MAC addre	ss: Technico_75:6d:af	(b0:c2:87:75:6d:af))				
	Sen	der IP addres	s: 192.168.0.1						
	Tar	get MAC addre	ss: IntelCor_d7:cf:76	(08:d4:0c:d7:cf:76))				
	Tar	get IP addres	s: 192.168.0.25						
									~
000	0 08	3 d4 0c d7 cf	76 b0 c2 87 75 6d af	08 06 00 01	.vum				
001	0 08	3 00 06 04 00	02 b0 c2 87 75 6d af	c0 a8 00 01	um.				
002	0 08	3 d4 0c d7 cf	76 c0 a8 00 19		v				
						11			
	🖉 Se	nder MAC address (a	rp.src.hw_mac), 6 bytes			Packets: 11804 · Displayed: 11804 (100.0	%)	Profile: De	efault 🔡

Slika 16 - Detaljan pregled paketa

Wireshark nudi spremanje i učitavanje snimljenih mrežnih paketa kako bi se mogli kasnije obrađivati. Kako bi se paketi spremili potrebno je zaustaviti njihovo snimanje pritiskom na crveni kvadrat u alatnoj traci te odabrati *File* \rightarrow *Save* i spremiti datoteku pod željenim imenom.



2.2.1 Filtriranje paketa

Kako broj paketa na mreži može biti jako velik, potreban je način za lakši pronalazak zanimljivih paketa. Jedna od glavnih značajki Wireshark-a koja služi upravo za to su filteri za prikaz odnosno snimanje paketa. Pakete je moguće filtrirati po IP adresama, protokolima, priključcima (eng. *ports*), sadržaju paketa i sl.

Jednostavan i često korišten primjer je filtriranje po IP adresama. Upisivanjem "ip.src == 93.184.216.34" u okvir za unos filtra u popisu paketa prikazuju se samo paketi kojima je izvorišna IP adresa 93.184.216.34. Ovakvo filtriranje paketa po izvorišnoj IP adresi prikazano je na slici 17.

	iFi				- 🗆 X
<u>F</u> ile <u>E</u>	dit <u>V</u> iew <u>G</u> o <u>C</u> ar	pture <u>A</u> nalyze <u>S</u> tatistics	Telephon <u>y W</u> ireless <u>T</u> oc	ols <u>H</u> elp	
	2017X	ି । 🔍 👄 🏟 🖉 有	🖢 📃 📃 Q, Q, Q, 🕅	1	
ip.src	== 93.184.216.34				Expression +
No.	Time	Source	Destination	Protocol	Length Info
	237 21.250242	93.184.216.34	192.168.0.25	ТСР	66 80 → 61954 [SYN, ACK] Sea=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK
	246 21.361924	93.184.216.34	192.168.0.25	TCP	60 80 → 61954 [ACK] Seq=1 Ack=365 Win=147456 Len=0
	247 21.362850	93.184.216.34	192.168.0.25	HTTP	1010 HTTP/1.1 200 OK (text/html)
	306 31.469430	93.184.216.34	192.168.0.25	ТСР	66 [TCP Keep-Alive ACK] 80 → 61954 [ACK] Seq=957 Ack=365 Win=14745
	371 41.577297	93.184.216.34	192.168.0.25	ТСР	66 [TCP Keep-Alive ACK] 80 → 61954 [ACK] Seq=957 Ack=365 Win=14745…
	415 51.684554	93.184.216.34	192.168.0.25	ТСР	66 [TCP Keep-Alive ACK] 80 → 61954 [ACK] Seq=957 Ack=365 Win=14745…
	462 61.791591	93.184.216.34	192.168.0.25	тср	66 [TCP Keep-Alive ACK] 80 → 61954 [ACK] Seq=957 Ack=365 Win=14745…
L	505 71.898894	93.184.216.34	192.168.0.25	тср	66 [TCP Keep-Alive ACK] 80 → 61954 [ACK] Seq=957 Ack=365 Win=14745…
> Fra	me 237: 66 byte	s on wire (528 bits)	, 66 bytes captured ((528 bits) o	n interface 0
> Eth	ernet II, Src:	Technico_75:6d:af (b	0:c2:87:75:6d:af), Ds	st: IntelCor	_d7:cf:76 (08:d4:0c:d7:cf:76)
> Int	ernet Protocol	Version 4, Src: 93.1	84.216.34, Dst: 192.1	168.0.25	_ , , ,
> Tra	nsmission Contr	ol Protocol, Src Por	t: 80, Dst Port: 6195	54, Seq: 0,	Ack: 1, Len: 0
0000	08 d4 0c d7 cf	76 b0 c2 87 75 6d	af 08 00 45 00	vum	.E.
0000 0010	08 d4 0c d7 cf 00 34 00 00 40	76 b0 c2 87 75 6d 00 36 06 4e 28 5d	af 08 00 45 00 b8 d8 22 c0 a8 .4	vum .@.6. N(]'	.E. "
0000 0010 0020	08 d4 0c d7 cf 00 34 00 00 40 00 19 00 50 f2	76 b0 c2 87 75 6d 00 36 06 4e 28 5d 02 4a a4 63 cf b6	af 08 00 45 00 b8 d8 22 c0 a8 .4 3f 2a 63 80 12f	vum .@.6. N(]' PJ. c?*(.E. " c
0000 0010 0020 0030	08 d4 0c d7 cf 00 34 00 00 40 00 19 00 50 f2 ff ff 6 f9 00 02 00	76 b0 c2 87 75 6d 00 36 06 4e 28 5d 02 4a a4 63 cf b6 00 02 04 05 b4 01	af 08 00 45 00 b8 d8 22 c0 a8 .4 3f 2a 63 80 12f 01 04 02 01 03	Vum .@.6. N(]' P.J. c?*(.E. * c
0000 0010 0020 0030 0040	08 d4 0c d7 cf 00 34 00 00 40 00 19 00 50 f2 ff ff f6 f9 00 03 09	76 b0 c2 87 75 6d 00 36 06 4e 28 5d 02 4a a4 63 cf b6 00 02 04 05 b4 01	af 08 00 45 00 b8 d8 22 c0 a8 .4 5f 2a 63 80 12 01 04 02 01 03	vum .@.6. N(]' PJ. c?*o	.E. * c.
0000 0010 0020 0030 0040	08 d4 0c d7 cf 00 34 00 00 40 00 19 00 50 f2 ff ff f6 f9 00 03 09	76 b0 c2 87 75 6d 00 36 06 4e 28 5d 02 4a a4 63 cf b6 00 02 04 05 b4 01	af 08 00 45 00 b8 d8 22 c0 a8 .4 3f 2a 63 80 12F 01 04 02 01 03	vum .@.6. N(]' P.J. c?*(.E. " c
0000 0010 0020 0030 0040	08 d4 0c d7 cf 00 34 00 00 40 00 19 00 50 f2 ff ff f6 f9 00 03 09	76 b0 c2 87 75 6d 00 36 06 4e 28 5d 02 4a a4 63 cf b6 00 02 04 05 b4 01	af 08 00 45 00 b8 d8 22 c0 a8 .4 3f 2a 63 80 12 01 04 02 01 03	vum @.6. N(]' P.J. c?*(.E. " C
0000 0010 0020 0030 0040	08 d4 0c d7 cf 00 34 00 00 40 00 19 00 50 f2 ff ff f6 f9 00 03 09	76 b0 c2 87 75 6d 00 36 06 4e 28 5d 02 4a a4 63 cf b6 00 02 04 05 b4 01	af 08 00 45 00 b8 d8 22 c0 a8 .4 3f 2a 63 80 12 01 04 02 01 03	vum .@.6. N(]' PJ. c?*(.E. " C
0000 0010 0020 0030 0040	08 d4 0c d7 cf 00 34 00 00 40 00 19 00 50 f2 ff ff f6 f9 00 03 09	76 b0 c2 87 75 6d 00 36 06 4e 28 5d 02 4a a4 63 cf b6 00 02 04 05 b4 01	af 08 00 45 00 b8 d8 22 c0 a8 .4 3f 2a 63 80 12 01 04 02 01 03	vum @.6. N(]' P.J. c?*(.E. " C
0000 0010 0020 0030 0040	08 d4 0c d7 cf 00 34 00 00 40 00 19 00 50 f2 ff ff f6 f9 00 03 09	76 b0 c2 87 75 6d 00 36 06 4e 28 5d 02 4a a4 63 cf b6 00 02 04 05 b4 01	af 08 00 45 00 b8 d8 22 c0 a8 .4 3f 2a 63 80 12 01 04 02 01 03	vum .@.6. N(]' PJ. c?*o	.E. * c.

Slika 17 – Filtriranje paketa po izvorišnoj IP adresi



2.2.2 Analiza DNS prometa

DNS (eng. *Domain Name System*) je sustav koji povezuje IP adrese sa simboličkim imenima koje je lakše pamtiti. Računala međusobno komuniciraju korištenjem IP adresa, tako da računalo mora simbolička imena (npr. *cert.hr*) prije korištenja prevesti u IP adresu. Taj proces prevođenja se odvija preko mreže te ga je moguće analizirati u Wireshark-u.

Upisivanjem teksta "dns" u polje za filtriranje u Wireshark-u prikazat će se samo DNS promet. Na slici 18 odabran je DNS upit, te je vidljivo polje upita tipa A kojim se traži IP adresa za simboličko ime *cert.hr*.

<u>,</u>	'WiFi																								_	[×	<
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>G</u> o	Capt	ure	Ana	alyze	e <u>S</u>	tatis	tics	Te	lep	nony	W	ireles	s i	Tools	s <u>H</u>	elp										
		0		Х	6	9		-		1	⊻			Œ		9	• •												
🔲 dn	s																							\times	-	💌 Exp	ressio	n	+
No.		Time			Sou	irce						De	stinat	ion				F	rotoc	ol	Lengt	h	Info						^
	4524	230.2	26505	9	83.	.139	9.10	03.3	3			19	2.1	68.6	0.25			D	NS		1	44	Star	ndar	rd	query	res	ро	
	4558	230.3	35864	1	192	2.16	58.6	0.25	5			83	.139	9.10	03.3			D	NS			77	Star	ndar	rd	query	0x7	74	
	4559	230.3	36754	6	83.	.139	9.10	03.3	3			19	2.1	68.6	9.25			D	NS		1	44	Star	ndar	٢d	query	res	ро	
	4749	238.8	37070	9	192	2.16	58.0	0.25	5			83	.139	9.10	03.3			D	NS			67	Star	ndar	٢d	query	0x2	da	
	4804	238.8	39304	9	83.	.139	9.10	03.3	3			19	2.1	68.0	9.25			D	ONS			83	Star	ndar	٢d	query	res	ро	
	4830	238.8	39520	7	192	2.16	58.0	0.25	5			83	.139	9.10	03.3			D	ONS			67	Star	ndar	rd	query	0xd	93	
-⊸	4869	238.9	91292	6	83.	.139	9.10	03.3	3			19	2.1	68.6	9.25			D	NS			83	Star	ndar	rd	query	res	ро	
	4870	238.9	91341	5	192	2.16	58.0	0.25	5			83	.139	9.10	03.3			D	NS			67	Star	ndar	٢d	query	0x1	.e0	
	4872	238.9	93151	9	83.	.139	9.10	03.3	3			19	2.10	68.0	9.25			D	NS		1	18	Star	ndar	rd	query	res	ро	~
:	[Re Tra Fla Que Ans Aut Add V Que	spons nsact gs: 0 stion wer R horit ition ries	e In: ion I x0100 s: 1 Rs: 0 y RRs al RR	48(D: () Sta) ;: 0 (s: (59] 0xd9: andar	37 rd (que	ry																					^
	>	cert.	nr:τ	ype	А, (clas	55.	TIN																					~
<																												>	
000 001 002 003 004	0 b0 0 00 0 67 0 00 0 01	0 c2 8 0 35 1 7 03 f 0 00 0 1 00 0	37 75 La e5 7 e5 90 00 91	6d 00 00	af 0 00 8 35 0 00 0	08 d 30 1 00 2 04 6	44 11 21	0c a4 69 65	d7 83 be 72	cf c0 d9 74	76 a8 37 02	08 00 01 68	00 19 00 72	45 53 00 00	00 8b 01 00	g	un 5 	n .5.!	i. ert	.v .7 t.hr	E. S.								
0	🗶 Те	xt item (text), 1	3 byte	s													Pa	ackets	: 578	3 · Dis	pla	yed: 1	138 (2	2.49	6) Pro	file: D	efaul	t

Slika 18 - Upit DNS prevoditelju



2.2.3 Analiza HTTP prometa

Protokol pomoću kojeg se prenose informacije na Webu naziva se HTTP (eng. *HyperText Transfer Protocol*). U HTTP protokolu podaci se razmjenjuju nešifrirani, tako da se korisnicima, kada god je to moguće, preporuča korištenje HTTPS protokola koji šifrira razmijenjene podatke. No, upravo zbog toga što podaci nisu šifrirani, u Wireshark-u je lako analizirati HTTP promet.

Upisivanjem teksta "http" u polje za filtriranje prikazat će se samo paketi koje je Wireshark prepoznao kao HTTP promet. Nakon posjeta Web stranice *example.org*, u Wiresharku je moguće vidjeti HTTP zahtjev i odgovor. Na slici 19 odabran je odgovor za detaljniji prikaz. Wireshark omogućuje interaktivan pregled polja karakterističnih za HTTP protokol. Tako je primjerice odabirom polja "File Data" moguće vidjeti HTML kod Web stranice.

File Go Capture Analyze Statistics lelephony Wireless Loois Help Image: Market and the state and
http Expression + No. Time Source Destination Protocol Length Info 67 7.908956 192.168.0.25 93.184.216.34 HTTP 484 GET / HTTP/1.1 69 8.016820 93.184.216.34 192.168.0.25 HTTP 1005 HTTP/1.1 200 OK (text
No. Time Source Destination Protocol Length Info • 67 7.908956 192.168.0.25 93.184.216.34 HTTP 484 GET / HTTP/1.1 - 69 8.016820 93.184.216.34 192.168.0.25 HTTP 1005 HTTP/1.1 200 OK (text
67 7.908956 192.168.0.25 93.184.216.34 HTTP 484 GET / HTTP/1.1 69 8.016820 93.184.216.34 192.168.0.25 HTTP 1005 HTTP/1.1 200 OK (text
- 69 8.016820 93.184.216.34 192.168.0.25 HTTP 1005 HTTP/1.1 200 OK (text
Vanue Accort Encoding >>>
Vary: Accept-Encoding\r\n
> Content-Length: 606\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.107864000 seconds]
<u>[Request in frame: 6/]</u>
File Data: 1270 bytes
<pre>> Line-based text data: text/html</pre>
0000 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a doctyp e html .
0010 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 <html>.< head>.</html>
0030 20 44 6f 6d 61 69 6e 3c 2f 74 69 74 6c 65 3e 0a Domain< /title>.
0040 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 . <me chars<="" ta="" td=""></me>
0050 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 et="utf- 8" />.
0060 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 <meta http-equ<="" td=""/>
0080 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f " content="text/
0090 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 html; ch arset=ut
Frame (1005 bytes) Uncompressed entity body (1270 bytes)
O Z File Data (http.file_data), 1270 bytes Packets: 502 · Displayed: 2 (0.4%) Profile: Default

Slika 19 - Odgovor Web poslužitelja



3 Zaključak

Wireshark je najpoznatiji besplatni alat za snimanje i analizu mrežnog prometa. On omogućuje detaljnu analizu velikog broja protokola te se razni IT stručnjaci svakodnevno služe njime. Mrežni arhitekti ga koriste za dizajniranje mrežnih protokola, sigurnosni stručnjaci za analizu sigurnosnih incidenata na mreži, programeri za implementaciju mrežnih protokola te ima još brojne primjene.

Wireshark je svoju primjenu našao i u edukaciji. Kako je Wireshark besplatan te se njegove osnovne značajke mogu koristiti bez puno predznanja, idealan je za upoznavanje s radom računalnih mreža.

U ovom dokumentu prikazane osnovne značajke alata Wireshark, no i one su već dovoljne za jednostavnu analizu velikog dijela mrežnog prometa.