Διαχείριση Δικτύων Τμήμα Μηχανικών ΤΕ ΤΕΙ Ηπείρου

Άσκηση εξοικείωσης με την εφαρμογή Wireshark

Η εφαρμογή Wireshark μας δίνει την δυνατότητα να συλλέξουμε όλη την δικτυακή κίνηση που μπορεί να γίνει αντιληπτή από τις επαφές δικτύου μας. Επίσης μας δίνει την δυνατότητα να επιθεωρήσουμε τα περιεχόμενα των πακέτων που στέλνονται ή λαμβάνονται από τον υπολογιστή μας. Εμείς θα την χρησιμοποιήσουμε σαν ένα μέσο για να γίνουν πιο κατανοητές ορισμένες έννοιες του μαθήματος όπως η ενθυλάκωση πακέτων και η λειτουργία των πρωτοκόλλων που εξετάζουμε.

[Μπορείτε να εγκαταστήσετε την εφαρμογή και στον προσωπικό σας υπολογιστή κατεβάζοντας την έκδοση που ταιριάζει από την σελίδα: <u>https://www.wireshark.org/#download]</u>

Διαδικασία Εξοικείωσης

Εμφανίστε την γραμμή εντολών για να την έχετε διαθέσιμη ώστε να δώσετε κάποια επιπλέον εντολή.

Στην συνέχεια ξεκινήστε την εφαρμογή Wireshark. Θα εμφανιστεί μια εικόνα όπως η παρακάτω

📕 The Wireshark Network Analyzer							
<u>File Edit Vi</u> ew <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics Telephon <u>y W</u> ireless <u>T</u> ools <u>H</u> elp							
M ■ 1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0							
Apply a display filter <ctrl-></ctrl->	Expression +						
Welcome to Wireshark Capture using this filter: Image:	•						
User's Guide Wiki Questions and Answers Mailing Lists							
You are running Wireshark 2.2.2 (v2.2.2-0-g775fb08). You receive automatic updates.							
Ready to load or capture No Packets	Profile: Default						

Στο κέντρο της σελίδας εμφανίζονται οι προσαρμογείς δικτύου για τους οποίους μπορούμε να συλλέξουμε κίνηση. Συνήθως θα μας ενδιαφέρει είτε μια σύνδεση Ethernet είτε μια ασύρματη

(wireless) σύνδεση. Επιλέξτε την Ethernet κάνοντας διπλό κλικ. Με τον τρόπο αυτό θα ξεκινήσει η συλλογή πακέτων και την σύνδεση που επιλέξατε και θα εμφανιστεί το ακόλουθο παράθυρο.

⊿ Ci	Capturing from Wireless Network Connection						
<u>F</u> ile	<u>E</u> dit <u>V</u> iew <u>G</u> o	<u>Capture</u> <u>A</u> nalyze <u>S</u> ta	tistics Telephon <u>y W</u> ireless	<u>T</u> ools <u>H</u> el	p		
	◢ ■ ◢ ◎						
	oply a display filter <	:Ctrl-/>			C	Expression +	
No.	Time	Source	Destination	Protocol L	ength Info	A	
	1 0.000000	192.168.1.254	224.0.0.1	IGMPv2	60 Membership Query, general		
	2 0.300128	192.168.1.3	224.0.0.252	IGMPv2	46 Membership Report group 224.0.0.	252	
	3 1.800112	192.168.1.3	239.255.255.250	IGMPv2	46 Membership Report group 239.255.	255.250	
	4 8.296019	192.168.1.3	224.0.0.251	IGMPv2	46 Membership Report group 224.0.0.	251	
	5 10.999860	192.168.1.254	224.0.0.12	IGMPv2	60 Membership Report group 224.0.0.	.12	
	6 14.999873	192.168.1.254	224.0.0.1	IGMPv2	60 Membership Query, general		
	7 16.171492	192.168.1.3	13.69.188.18	TLSv1.2	155 Application Data		
•	0 10 071004	13 60 100 10	102 102 1 2	TLC1 0	AFF ALLIILLIL DILL		
D F	came 1: 60 bytes	on wire (480 hits)	60 bytes centured (480	hits) on i	nterface 0		
ÞE	thernet II. Src:	ZteCorpo cc:72:e8 (cc:7b:35:cc:72:e8). Dst	: IntelCor	1d:6c:14 (00:21:6a:1d:6c:14)		
ÞI	nternet Protocol	Version 4, Src: 192	2.168.1.254, Dst: 224.0.0	0.1			
ÞI	nternet Group Ma	nagement Protocol	,				
\bigcirc	Wireless Network	Connection: <live capture="" ir<="" td=""><td>n progress></td><td></td><td>Packets: 10 · Displayed: 10 (100.0%)</td><td>Profile: Default</td></live>	n progress>		Packets: 10 · Displayed: 10 (100.0%)	Profile: Default	

Θα παρατηρήσετε ότι στο πάνω μέρος του εσωτερικού παραθύρου εμφανίζεται ένας πίνακας με γραμμές. Κάθε μια αντιπροσωπεύει ένα πλαίσιο που έγινε αντιληπτό από την εφαρμογή.

Ενώ τρέχει η εφαρμογή δώστε στην γραμμή εντολών μια εντολή ping για παράδειγμα:

ping www.yahoo.com

Θα παρατηρήσετε ότι στο παράθυρο της εφαρμογής εμφανίζονται κάποια νέα πακέτα που αντιπροσωπεύουν τα μηνύματα ICMP Echo Request και Echo Reply που στέλνει και λαμβάνει η εντολή ping, όπως φαίνονται στην ακόλουθη εικόνα.

	*Wireless Network Connection					
<u>F</u> ile	<u>E</u> dit <u>V</u> iew <u>G</u> o	<u>Capture</u> <u>Analyze</u> <u>Stati</u>	stics Telephon <u>y W</u> ireless	<u>T</u> ools <u>H</u>	<u>d</u> elp	
	🔳 🧟 🛞 🔚 🔚	🔀 🖸 । ९ 🗢 🔿 🕾	👔 🛓 🚆 🗐 🍳 Q	Q. 🎹		
	Apply a display filter <	Ctrl-/>			🖘 🕤 Expression 🕇	
No.	Time	Source	Destination	Protocol	Length Info	
	51 64.793341	192.168.1.3	224.0.0.251	IGMPv2	46 Membership Report group 224.0.0.251	
	52 69.571084	192.168.1.3	192.168.1.254	DNS	72 Standard query 0x0b98 A www.yahoo.gr	
	53 69.606138	192.168.1.254	192.168.1.3	DNS	295 Standard query response 0x0b98 A www.yahoo.gr	
-	54 69.611140	192.168.1.3	77.238.184.150	ICMP	74 Echo (ping) request id=0x0001, seq=1/256, tt	
	55 69.710893	77.238.184.150	192.168.1.3	ICMP	74 Echo (ping) reply id=0x0001, seq=1/256, tt	
	56 70.623285	192.168.1.3	77.238.184.150	ICMP	74 Echo (ping) request id=0x0001, seq=2/512, tt	
	57 70.727577	77.238.184.150	192.168.1.3	ICMP	74 Echo (ping) reply id=0x0001, seq=2/512, tt	
	58 70.999520	192.168.1.254	224.0.0.12	IGMPv2	60 Membership Report group 224.0.0.12	
	59 71.174000	192.168.1.3	13.69.188.18	TLSv1.2	155 Application Data	
	60 71.274119	13.69.188.18	192.168.1.3	TLSv1.2	155 Application Data	
	61 71.473318	192.168.1.3	13.69.188.18	TCP	54 62980→443 [ACK] Seq=203 Ack=203 Win=4200 Len=	
	62 71.623424	192.168.1.3	77.238.184.150	ICMP	74 Echo (ping) request id=0x0001, seq=3/768, tt	
	63 71.723863	77.238.184.150	192.168.1.3	ICMP	74 Echo (ping) reply id=0x0001, seq=3/768, tt	
	64 72.623478	192.168.1.3	77.238.184.150	ICMP	74 Echo (ping) request id=0x0001, seq=4/1024, t	
	65 72.723602	77.238.184.150	192.168.1.3	ICMP	74 Echo (ping) reply id=0x0001, seq=4/1024, t	
	66 75.000794	192.168.1.254	224.0.0.1	IGMPv2	60 Membership Query, general	
	67 75 75/750	102 168 1 3	65 55 223 27	HIND	73 518640033 an-31	
Frame 54: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0 Ethernet II, Src: IntelCor_1d:6c:14 (00:21:6a:1d:6c:14), Dst: ZteCorpo_cc:72:e8 (cc:7b:35:cc:72:e8) Internet Protocol Version 4, Src: 192.168.1.3, Dst: 77.238.184.150 Internet Control Message Protocol						
⊘ Z wireshark_A529BC1E-9DDD-4266-AE6E-4643941C95BC_20171008155948_a05264						

Στο σημείο αυτό μπορούμε να διακόψουμε την συλλογή πακέτων πατώντας το κόκκινο κουμπί που βρίσκεται πάνω αριστερά κάτω από το μενού εντολών.

Στο κάτω τμήμα του παραθύρου βρίσκεται η περιοχή που εμφανίζει λεπτομέρειες για κάθε πλαίσιο που επιλέγεται στην πάνω λίστα. Υπάρχουν διαφορετικές περιοχές στις οποίες μπορείτε να εξετάζεται πληροφορίες που τοποθετούνται από τα πρωτόκολλα διαφορετικών επιπέδων. Μπορείτε να βλέπετε αυτές τις πληροφορίες ανοίγοντας τις αντίστοιχες καρτέλες.

	*Wireless Network Connection							
Eil	e <u>E</u> dit <u>V</u> iew <u>G</u> o	<u>Capture Analyze Stat</u>	stics Telephon <u>y W</u> ireles	s <u>T</u> ools <u>I</u>	Help			
	📶 🔲 🖉 💿 🕌 🚵 🖄 🔍 🗢 🕾 🗑 🖢 🚍 🗐 🍳 Q. Q. 🕱 🎹							
	Apply a display filter <	:Ctrl-/>			Expression	÷		
No.	Time	Source	Destination	Protocol	I Length Info	*		
	51 64.793341	192.168.1.3	224.0.0.251	IGMPv2	2 46 Membership Report group 224.0.0.251			
	52 69.571084	192.168.1.3	192.168.1.254	DNS	72 Standard query 0x0b98 A www.yahoo.gr			
	53 69.606138	192.168.1.254	192.168.1.3	DNS	295 Standard query response 0x0b98 A www.yahoo.gr			
-	54 69.611140	192.168.1.3	77.238.184.150	ICMP	74 Echo (ping) request id=0x0001, seq=1/256, tt			
	55 69.710893	77.238.184.150	192.168.1.3	ICMP	74 Echo (ping) reply id=0x0001, seq=1/256, tt			
	56 70.623285	192.168.1.3	77.238.184.150	ICMP	74 Echo (ping) request id=0x0001, seq=2/512, tt			
	57 70.727577	77.238.184.150	192.168.1.3	ICMP	74 Echo (ping) reply id=0x0001, seq=2/512, tt	-		
•								
⊳	Frame 54: 74 byte	s on wire (592 bits)	74 bytes captured (5	92 bits) o	on interface 0			
4	Ethernet II, Src:	IntelCor_1d:6c:14 (0	0:21:6a:1d:6c:14), Ds	t: ZteCorp	<pre>'po_cc:72:e8 (cc:7b:35:cc:72:e8)</pre>			
	A Destination: Z	teCorpo_cc:72:e8 (cc:	7b:35:cc:72:e8)					
	Address: Zto	eCorpo_cc:72:e8 (cc:7	b:35:cc:72:e8)					
	0	=	LG bit: Globally uniq	ue address	s (factory default)			
	0 = IG bit: Individual address (unicast)							
	4 Source: IntelCor_1d:6c:14 (00:21:6a:1d:6c:14)							
	Address: In	telCor_1d:6c:14 (00:2	1:6a:1d:6c:14)			-		
	0 = IG bit: Individual address (unicast)							
	Type: IPv4 (0x	0800)	460 4 3 Date 77 030	104 150				
	P Internet Protocol Version 4, Src: 192.168.1.3, Dst: 77.238.184.150							
1	Internet Control Message Protocol							
	Type: 8 (Echo	(ping) request)						
	Code: 0							
	[Checksum Stat	us: Good]						
	Identifier (BE): 1 (0x0001)				-		
C) 📝 Frame is ignored	by the dissectors (frame.ignor	ed)		Packets: 71 · Displayed: 71 (100.0%) Profile: Default			

Τέλος μπορείτε να εμφανίσετε την σειρά byte του επιλεγμένου πακέτου επιλέγοντας View->Packet Bytes

Τερματίστε την εφαρμογή επιλέγοντας Stop and Quit Without Saving.