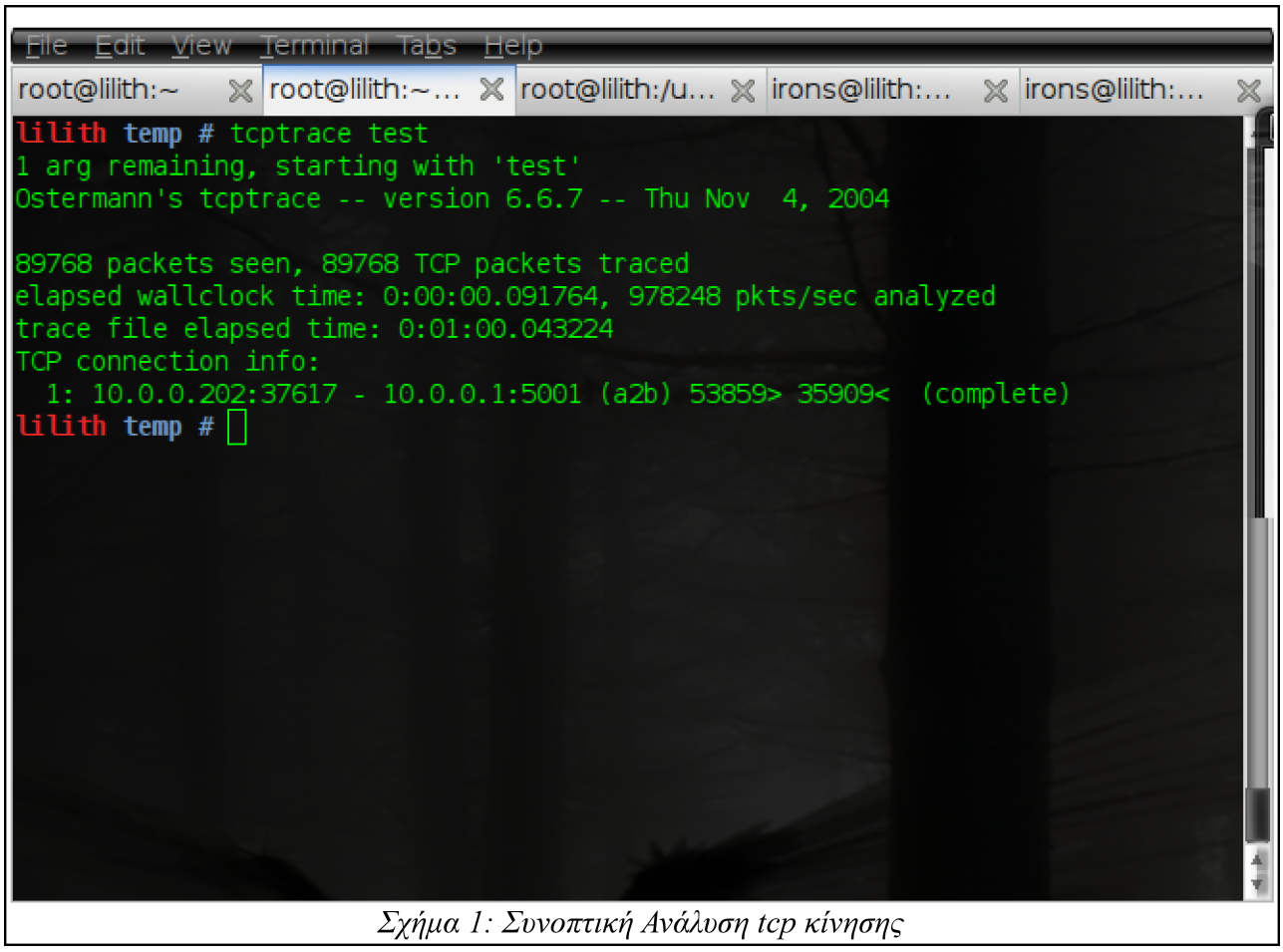
ΑΝΑΛΥΣΗ TCP ΚΙΝΗΣΗΣ ΜΕ ΤΟ ΠΡΟΓΡΑΜΜΑ TCPTRACE.

ΔΕΔΟΜΕΝΑ

tcptrace: είναι το όνομα της εντολής ανάλυσης της tcp κίνησης.
test: είναι το όνομα του tcpdump αρχείου.
detailed_analysis: είναι το όνομα του txt αρχείου στο οποίο αποθηκεύεται η λεπτομερής ανάλυση.
traffic_bytes.xpl: είναι το αρχείο που κρατάει πληροφορίες για τη γραφική του ρυθμού μετάδοσης δεδομένων (το δίνει το tcptrace).
traffic_rtt.xpl: είναι το αρχείο που κρατάει πληροφορίες για τη γραφική του RTT (το δίνει το tcptrace).
traffic_loss.xpl: είναι το αρχείο που κρατάει πληροφορίες για τη γραφική των επανεκπομπών (το δίνει το tcptrace).
a2b_owin.xpl: είναι το αρχείο που κρατάει πληροφορίες για τη γραφική των ανεπιβεβαίωτων δεδομένων από το υπολογιστή a στο b.
xplot: είναι η εντολή εμφάνισης των γραφικών που δίνει το tcptrace.

Συνοπτική Ανάλυση TCP Κίνησης

Εντολή: **tcptrace test**



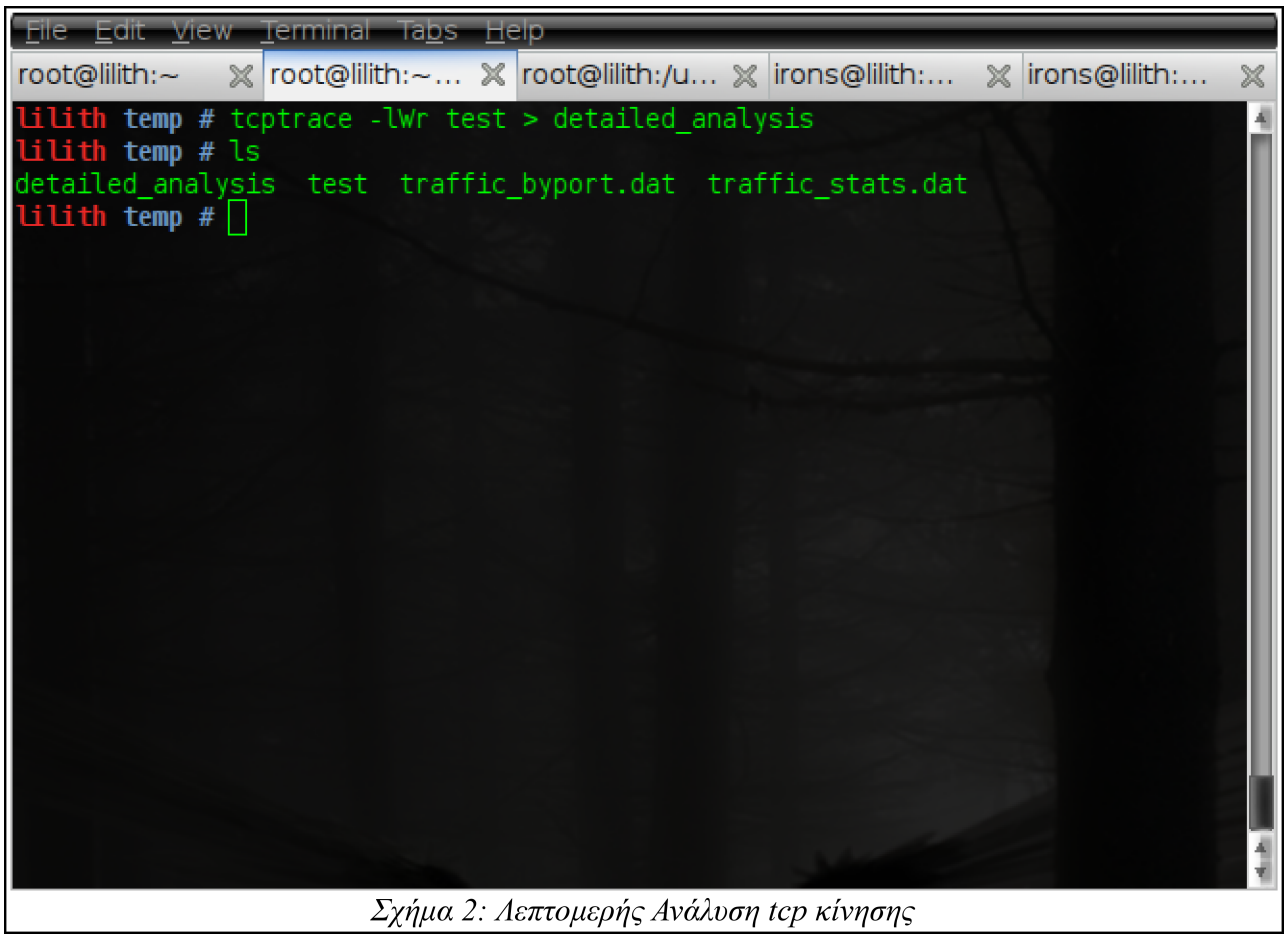
Σχήμα 1: Συνοπτική Ανάλυση tcp κίνησης

Από τη συνοπτική ανάλυση μπορούμε να δούμε ότι έχουμε 1 tcp σύνδεση μεταξύ των

υπολογιστών a με IP:port 10.0.0.202:37617 και b με IP:port 10.0.0.1:5001. Ο a έστειλε 53859 tcp segments ενώ ο b 35909 tcp segments.

Λεπτομερής Ανάλυση TCP Κίνησης

Εντολή: **tcptrace -lWr test > detailed_analysis**



Σχήμα 2: Λεπτομερής Ανάλυση tcp κίνησης

Το αρχείο detailed_analysis μπορούμε να το δούμε με έναν απλό text editor. Παρακάτω δίδονται τα περιεχόμενου του εν λόγω αρχείου.

1 arg remaining, starting with 'test'
Ostermann's tcptrace -- version 6.6.7 -- Thu Nov 4, 2004

89768 packets seen, 89768 TCP packets traced
elapsed wallclock time: 0:00:00.095941, 935658 pkts/sec analyzed
trace file elapsed time: 0:01:00.043224
TCP connection info:
1 TCP connection traced:
TCP connection 1:

host a: 10.0.0.202:37617
host b: 10.0.0.1:5001
complete conn: yes

first packet: Mon Apr 19 16:38:27.814297 2010
last packet: Mon Apr 19 16:39:27.857522 2010
elapsed time: 0:01:00.043224
total packets: 89768
filename: test

a->b:		b->a:	
total packets:	53859	total packets:	35909
ack pkts sent:	53858	ack pkts sent:	35909
pure acks sent:	2	pure acks sent:	35907
sack pkts sent:	0	sack pkts sent:	0
dsack pkts sent:	0	dsack pkts sent:	0
max sack blks/ack:	0	max sack blks/ack:	0
unique bytes sent:	77979672	unique bytes sent:	0
actual data pkts:	53856	actual data pkts:	0
actual data bytes:	77979672	actual data bytes:	0
rexmt data pkts:	0	rexmt data pkts:	0
rexmt data bytes:	0	rexmt data bytes:	0
zwnd probe pkts:	0	zwnd probe pkts:	0
zwnd probe bytes:	0	zwnd probe bytes:	0
outoforder pkts:	0	outoforder pkts:	0
pushed data pkts:	4544	pushed data pkts:	0
SYN/FIN pkts sent:	1/1	SYN/FIN pkts sent:	1/1
req 1323 ws/ts:	Y/Y	req 1323 ws/ts:	Y/Y
adv wind scale:	6	adv wind scale:	0
req sack:	Y	req sack:	Y
sacks sent:	0	sacks sent:	0
urgent data pkts:	0 pkts	urgent data pkts:	0 pkts
urgent data bytes:	0 bytes	urgent data bytes:	0 bytes
mss requested:	1460 bytes	mss requested:	1460 bytes
max segm size:	1448 bytes	max segm size:	0 bytes
min segm size:	24 bytes	min segm size:	0 bytes
avg segm size:	1447 bytes	avg segm size:	0 bytes
max win adv:	5888 bytes	max win adv:	17376 bytes
min win adv:	5888 bytes	min win adv:	11584 bytes
zero win adv:	0 times	zero win adv:	0 times
avg win adv:	5888 bytes	avg win adv:	16650 bytes
max owin:	17377 bytes	max owin:	1 bytes
min non-zero owin:	1 bytes	min non-zero owin:	1 bytes
avg owin:	16405 bytes	avg owin:	1 bytes
wavg owin:	16226 bytes	wavg owin:	0 bytes
initial window:	2920 bytes	initial window:	0 bytes
initial window:	3 pkts	initial window:	0 pkts
ttl stream length:	77979672 bytes	ttl stream length:	0 bytes
missed data:	0 bytes	missed data:	0 bytes
truncated data:	76687128 bytes	truncated data:	0 bytes
truncated packets:	53855 pkts	truncated packets:	0 pkts
data xmit time:	60.031 secs	data xmit time:	0.000 secs
idletime max:	40.0 ms	idletime max:	40.0 ms
throughput:	1298726 Bps	throughput:	0 Bps
RTT samples:	35883	RTT samples:	2

RTT min:	1.4 ms	RTT min:	0.0 ms
RTT max:	54.3 ms	RTT max:	0.0 ms
RTT avg:	12.6 ms	RTT avg:	0.0 ms
RTT stdev:	3.1 ms	RTT stdev:	0.0 ms
RTT from 3WHS:	1.4 ms	RTT from 3WHS:	0.0 ms
RTT full_sz smpls:	35881	RTT full_sz smpls:	1
RTT full_sz min:	5.0 ms	RTT full_sz min:	0.0 ms
RTT full_sz max:	54.3 ms	RTT full_sz max:	0.0 ms
RTT full_sz avg:	12.6 ms	RTT full_sz avg:	0.0 ms
RTT full_sz stdev:	3.1 ms	RTT full_sz stdev:	0.0 ms
post-loss acks:	0	post-loss acks:	0
segs cum acked:	17974	segs cum acked:	0
duplicate acks:	0	duplicate acks:	0
triple dupacks:	0	triple dupacks:	0
max # retrans:	0	max # retrans:	0
min retr time:	0.0 ms	min retr time:	0.0 ms
max retr time:	0.0 ms	max retr time:	0.0 ms
avg retr time:	0.0 ms	avg retr time:	0.0 ms
sdv retr time:	0.0 ms	sdv retr time:	0.0 ms

Περιγραφή Πεδίων του αρχείου detailed_analysis.

Από τη ανάλυση μπορούμε να δούμε ότι έχουμε 1 tcp σύνδεση μεταξύ των υπολογιστών a με IP:port 10.0.0.202:37617 και b με IP:port 10.0.0.1:5001.
Υπάρχουν δύο στήλες μία για τη κίνηση από το a στο b και μια για τη κίνηση από το b στο a.

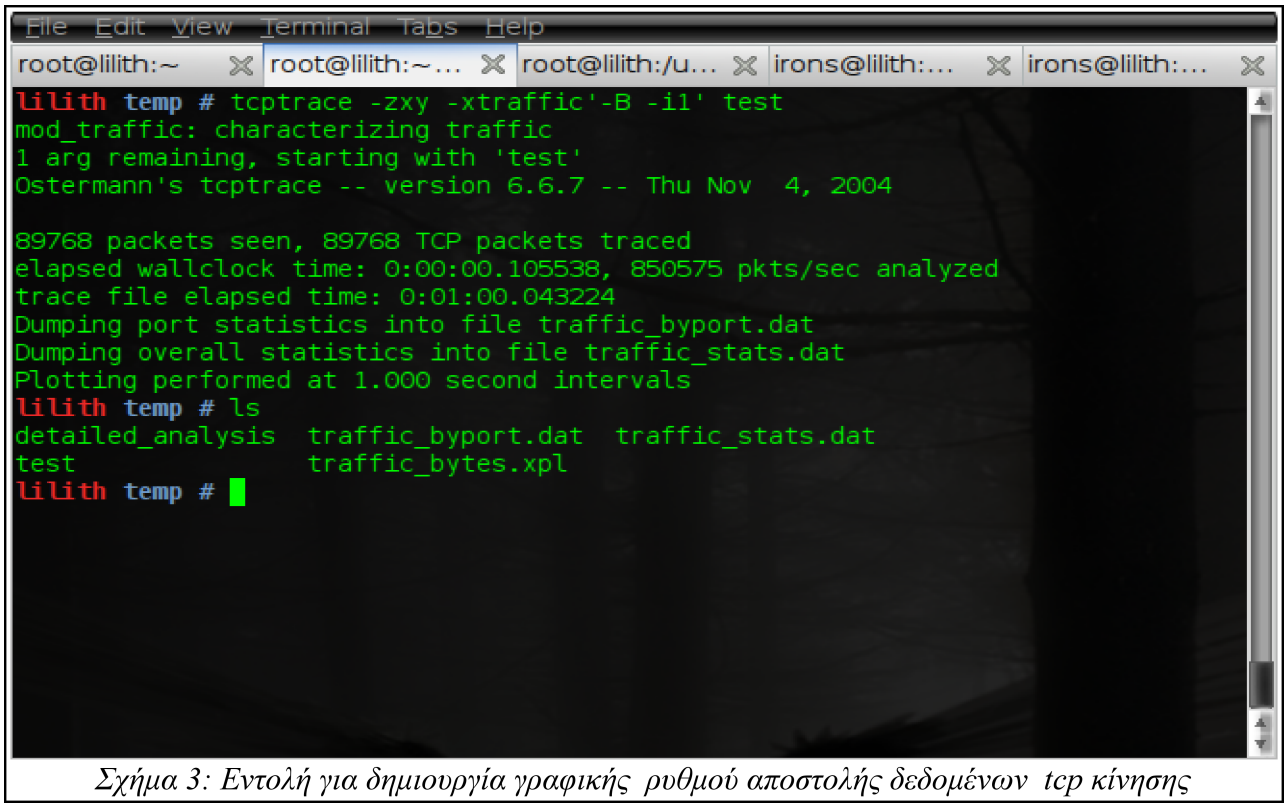
- total packets: Ο συνολικός αριθμός των πακέτων.
- ack pkts sent: Ο συνολικός αριθμός των επιβεβαιώσεων.
- pure acks sent: Ο συνολικός αριθμός των καθαρών επιβεβαιώσεων.
- sack pkts sent: Ο συνολικός αριθμός των επιλεκτικών επιβεβαιώσεων.
- dsack pkts sent: Ο συνολικός αριθμός των διπλών επιλεκτικών επιβεβαιώσεων.
- max sack blks/ack: Ο μέγιστος αριθμός κομματιών που επιβεβαίωνε μια SACK επιβεβαίωση.
- unique bytes sent: Ο αριθμός των μεταδιδόμενων bytes χωρίς να έχουν μετρηθεί τα bytes τυχόν επανεκπομπών.
- actual data pkts : Ο αριθμός όλων των πακέτων με τουλάχιστον ένα byte ωφέλιμο φορτίο.
- actual data bytes: Ο αριθμός όλων των μεταδιδόμενων bytes (μαζί και τα bytes τυχόν επανεκπομπών).
- rexmt data pkts: Ο αριθμό των επανεκπεμπόμενων πακέτων.
- rexmt data bytes: Ο αριθμό των επανεκπεμπόμενων bytes.
- zwnd probe pkts: Ο αριθμός των πακέτων διερεύνησης παραθύρου (στέλνονται για να ανακαλυφθεί εάν ο παραλήπτης έχει ξανανοίξει το παράθυρο του).
- zwnd probe bytes: Ο αριθμός σε bytes των δεδομένων που ήταν μέσα στα πακέτα διερεύνησης παραθύρου.
- outoforder pkts: Ο αριθμός όλων των πακέτων που έφτασαν εκτός σειράς.
- pushed data pkts: Ο αριθμός όλων των πακέτων με το PUSH bit ενεργοποιημένο.

- SYN/FIN pkts sent: Ο αριθμός όλων των πακέτων με τα SYN/FIN bits ενεργοποιημένα.
- req 1323 ws/ts: Υποδεικνύει εάν έχει ζητηθεί η ενεργοποίηση για Window Scaling/Time Stamp όπως ορίζεται στον RFC 1323. Ένα `Y' φανερώνει ενεργοποίηση ένα `N' το αντίθετο.
- adv wind scale: Ο παράγων αύξησης του παραθύρου.
- req sack: Υποδεικνύει εάν έχει ζητηθεί η ενεργοποίηση για SACK. Ένα `Y' φανερώνει ενεργοποίηση ένα `N' το αντίθετο.
- sacks sent: Ο συνολικός αριθμός των ACK πακέτων που μετέφεραν SACK πληροφορία.
- urgent data pkts: Ο αριθμός όλων των πακέτων με το URG bit ενεργοποιημένο .
- urgent data bytes: Ο αριθμός όλων των urgent bytes .
- mss requested: Το Maximum Segment Size (MSS) που ζητήθηκε σαν TCP επιλογή στο SYN πακέτο της σύνδεσης.
- max segm size: Το Maximum Segment Size (MSS) που παρατηρήθηκε στη διάρκεια της σύνδεσης.
- min segm size: Το minimum segment size που παρατηρήθηκε στη διάρκεια της σύνδεσης.
- avg segm size: Το average segment size που παρατηρήθηκε στη διάρκεια της σύνδεσης.
- max win adv: Το maximum window advertisement που παρατηρήθηκε στη διάρκεια της σύνδεσης.
- min win adv: Το minimum window advertisement που παρατηρήθηκε στη διάρκεια της σύνδεσης.
- zero win adv: Το πλήθος των πακέτων με τιμή 0 στο window πεδίο.
- avg win adv: Το μέσο window advertisement που παρατηρήθηκε στη διάρκεια της σύνδεσης.
- max owin: Ο μέγιστος αριθμός (bytes) ανεπιβεβαίωτων δεδομένων που παρατηρήθηκαν κατά τη διάρκεια της σύνδεσης.
- min non-zero owin: Ο ελάχιστος αριθμός (bytes) ανεπιβεβαίωτων δεδομένων που παρατηρήθηκαν κατά τη διάρκεια της σύνδεσης.
- avg owin: Ο μέσος όρος (bytes) των ανεπιβεβαίωτων δεδομένων που παρατηρήθηκαν κατά τη διάρκεια της σύνδεσης.
- wavg owin: Ο εξομαλυνθείς μέσος όρος (bytes) των ανεπιβεβαίωτων δεδομένων που παρατηρήθηκαν κατά τη διάρκεια της σύνδεσης.
- initial window: Το αρχικό window της σύνδεσης (bytes).
- initial window: Το αρχικό window της σύνδεσης (segments).
- ttl stream length: Τα συνολικά bytes της σύνδεσης όπως προκυπτουν από την αφαίρεση του ISN και του τελικού SN (FIN πακέτο).
- missed data: Η διαφορά μεταξύ του ttl stream length και των unique bytes sent.
- truncated data: Ο αριθμός των συγχωνευμένων bytes.
- truncated packets: Ο αριθμός των συγχωνευμένων πακέτων..
- data xmit time: Ο χρόνο μετάδοσης των δεδομένων.
- idletime max: Ο Maximum χρόνο αναμονής μεταξύ δύο διαδοχικών πακέτων.
- throughput: Το μέσο throughput.
- RTT samples: Ο Αριθμός των έγκυρων RTT δειγμάτων (δεν παίρνεται υπόψη το RTT επανεκπεμπόμενων πακέτων).
- RTT min: Το minimum RTT.
- RTT max: Το maximum RTT.
- RTT avg: Το μέσο RTT.
- RTT stdev: Η τυπική απόκλιση του RTT.
- RTT from 3WHS: Το RTT του 3-Way Hand-Shake.
- RTT full_sz smpls: Ο αριθμός των RTT δειγμάτων με πλήρες μέγεθος.

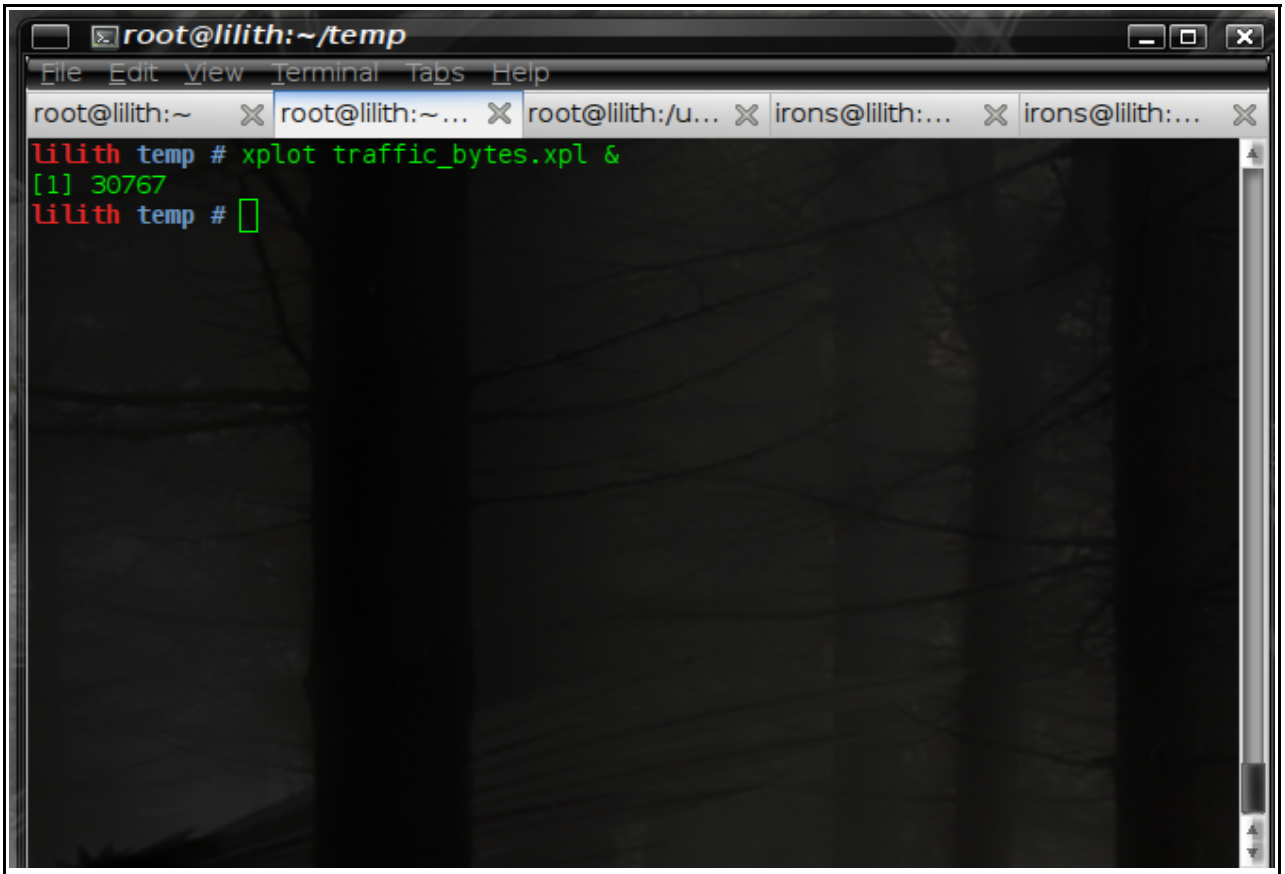
- RTT full_sz min: Το minimum RTT δειγμάτων με πλήρες μέγεθος.
- RTT full_sz max: Το maximum RTT δειγμάτων με πλήρες μέγεθος.
- RTT full_sz avg: Το μέσο RTT δειγμάτων με πλήρες μέγεθος.
- RTT full_sz stdev: Η τυπική απόκλιση του RTT δειγμάτων με πλήρες μέγεθος.
- post-loss acks: Ο αριθμός των επιβεβαιώσεων που λήφθηκαν ενώ ένα τουλάχιστον segment που επιβεβαίωναν έχει επανεκπεμπεί.
- ambiguous acks, RTT min, RTT max, RTT avg, RTT sdv: Τα πεδία αυτά εμφανίζονται εάν έχουμε την περίπτωση αμφισημίας επιβεβαιώσεων. Εμφανίζεται ο αριθμός των επιβεβαιώσεων αυτών καθώς και το RTT τους. Ο χρόνος υπολογίζεται βάση του τελευταίου επανεκπεμπόμενου πακέτου.
- segs cum acked: Ο αριθμός των segments που επιβεβαιώθηκαν όχι απευθείας αλλά λόγω του συσσωρευτικού τρόπου λειτουργίας των ACK.
- duplicate acks: Ο συνολικός αριθμός των διπλών επιβεβαιώσεων για τα ληφθέντα segment.
- triple dupacks: Ο συνολικός αριθμός των τρείς φορές διπλών επιβεβαιώσεων για κάποιο segment (ενεργοποιεί το fast-retransmit/fast-recovery μηχανισμό).
- max # retrans: Ο μέγιστος αριθμός επανεκπομπών που παρατηρήθηκε στη διάρκεια της σύνδεσης.
- min retr time: Ο minimum χρόνος μεταξύ δύο επανεκπομπών για όλες τις επανεκπομπές που παρατηρήθηκαν.
- max retr time: Ο maximum χρόνος μεταξύ δύο επανεκπομπών για όλες τις επανεκπομπές που παρατηρήθηκαν.
- avg retr time: Ο μέσος χρόνος μεταξύ δύο επανεκπομπών για όλες τις επανεκπομπές που παρατηρήθηκαν.
- sdv retr time: Η τυπική απόκλιση των επανεκπομπών.

Γραφική ρυθμού αποστολής δεδομένων TCP Κίνησης

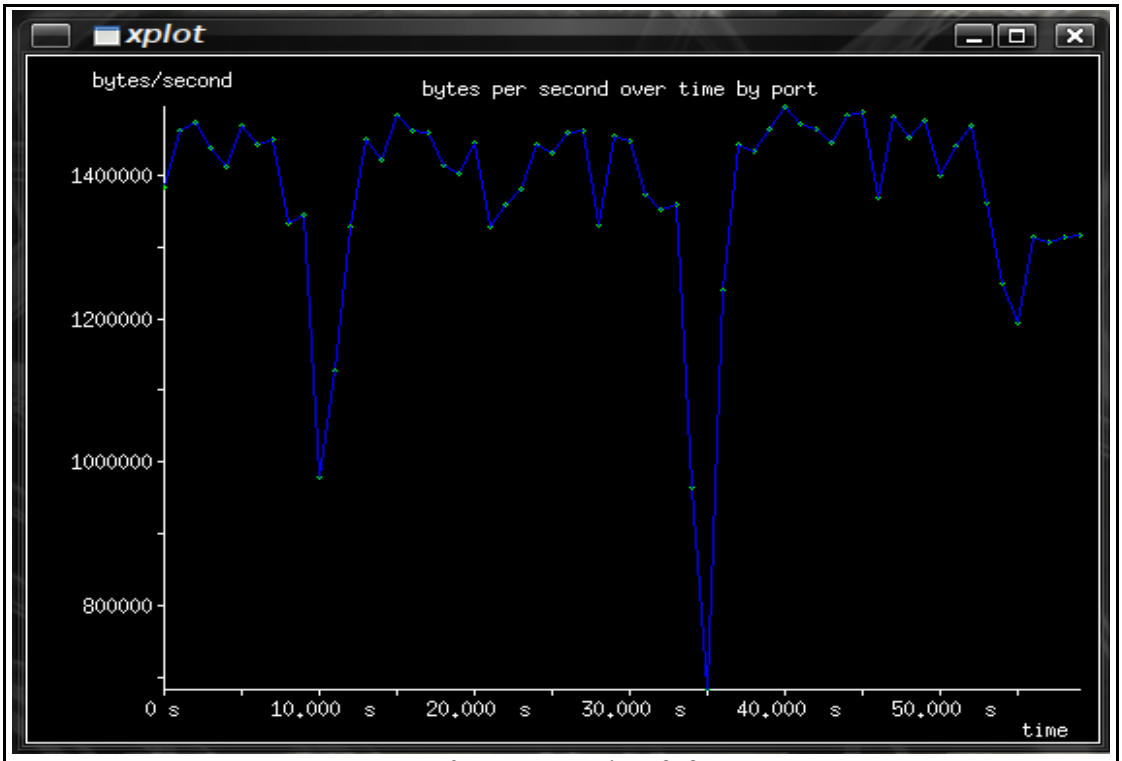
Εντολή: **tcptrace -zxy -xtraffic'-B -i1' test, όπου το -i καθορίζει το χρόνο δειγματοληψίας.**



Σχήμα 3: Εντολή για δημιουργία γραφικής ρυθμού αποστολής δεδομένων tcp κίνησης



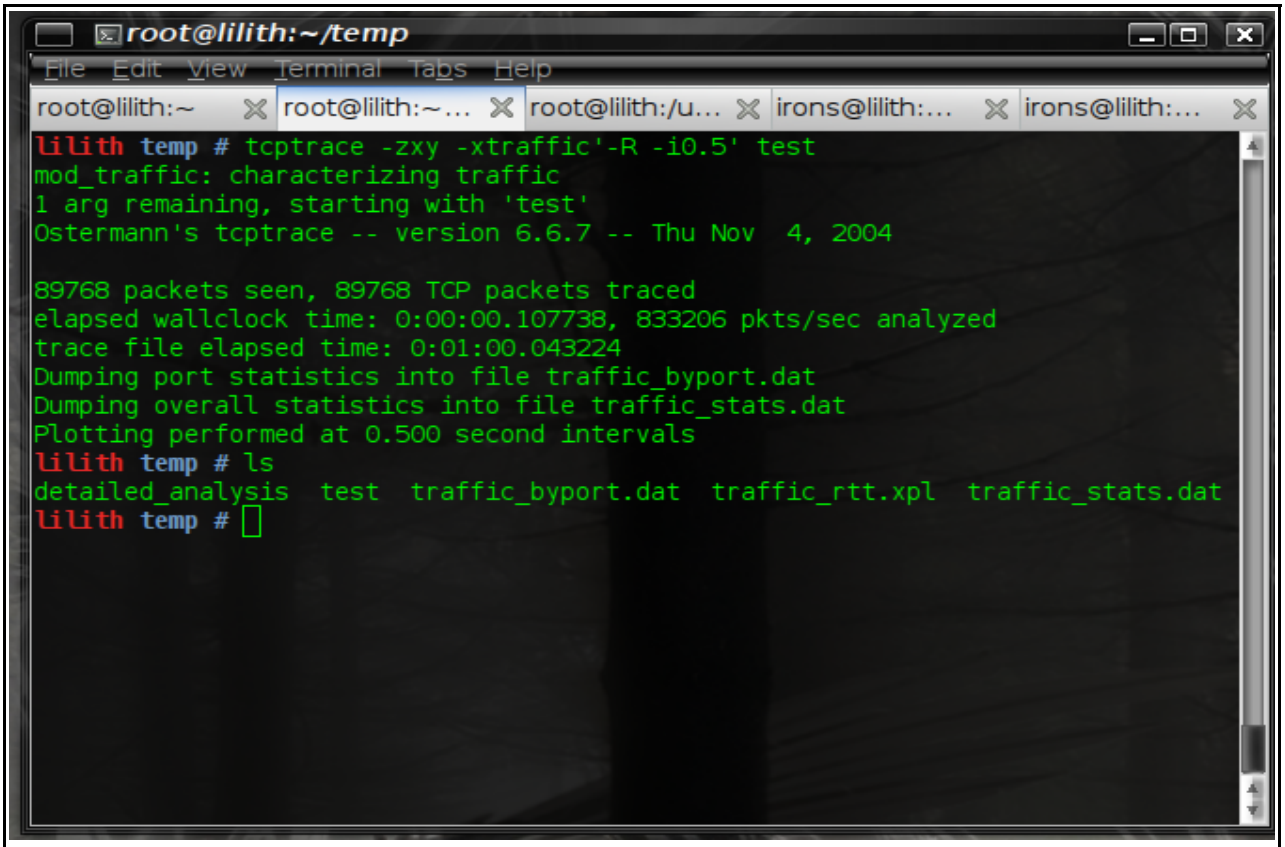
Σχήμα 4: Εντολή για εμφάνιση γραφικής ρυθμού αποστολής δεδομένων tcp κίνησης



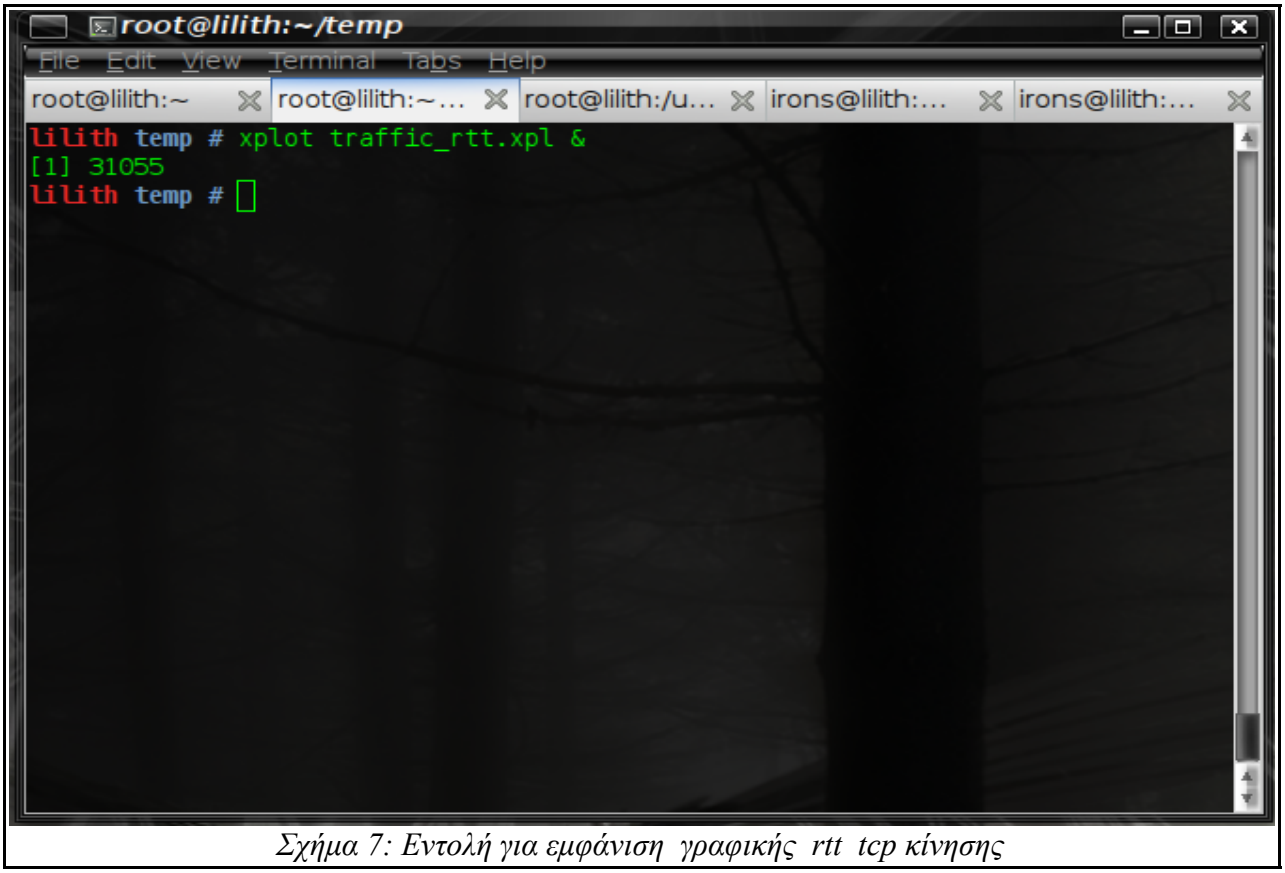
Σχήμα 5: Γραφική ρυθμού αποστολής δεδομένων tcp κίνησης

Γραφική Round Trip Time TCP Κίνησης

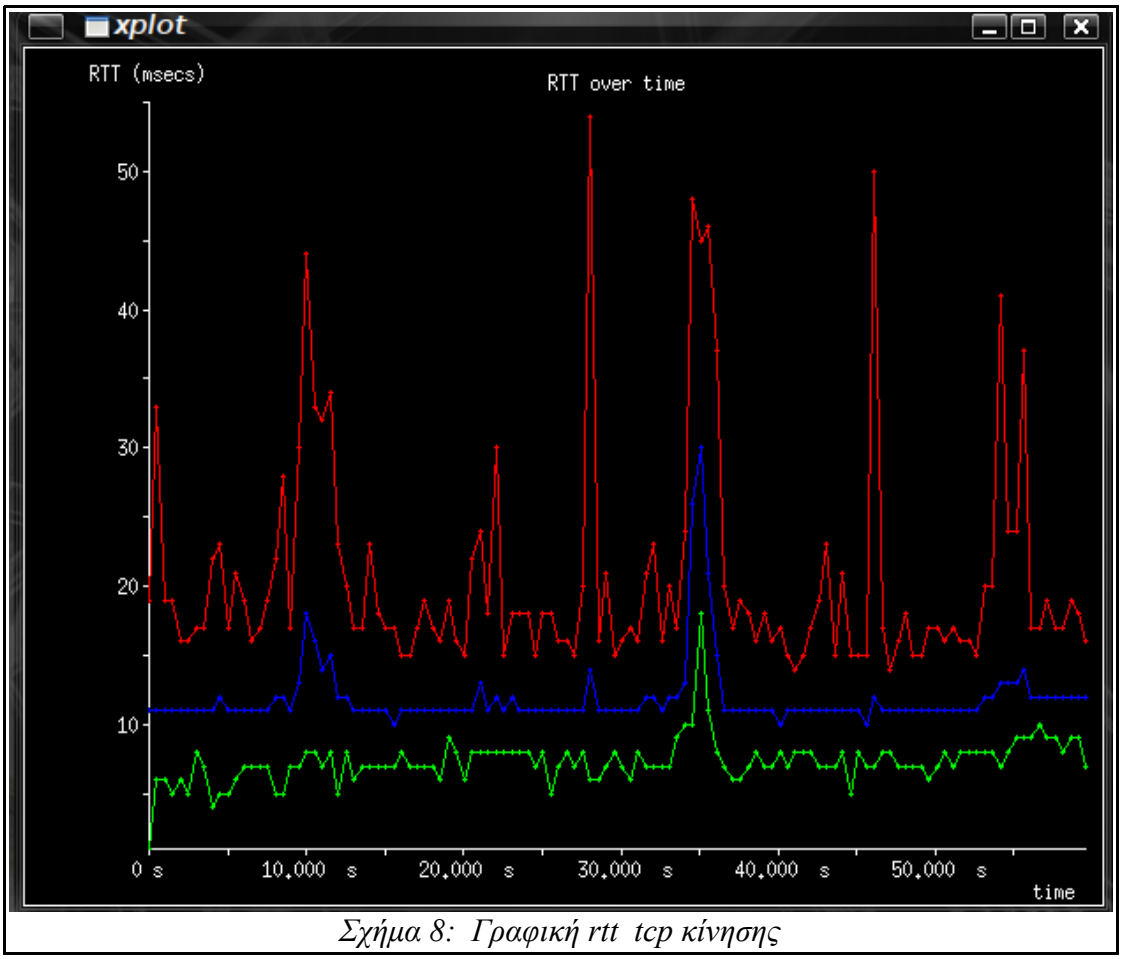
Εντολή: **tcptrace -zxy -xtraffic'-R -i0.5' test, όπου το -i καθορίζει το χρόνο δειγματοληψίας.**



Σχήμα 6: Εντολή για δημιουργία γραφικής rtt tcp κίνησης



Σχήμα 7: Εντολή για εμφάνιση γραφικής rtt tcp κίνησης

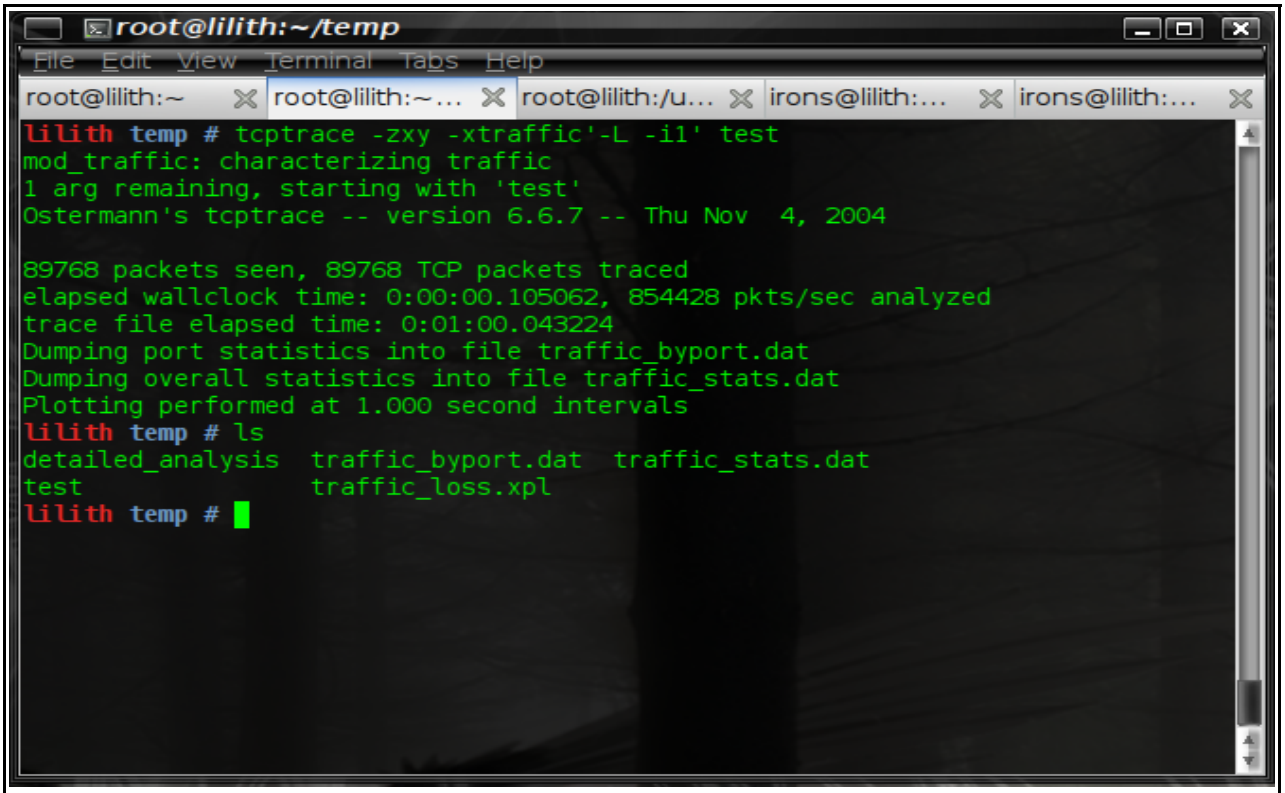


Σχήμα 8: Γραφική rtt tcp κίνησης

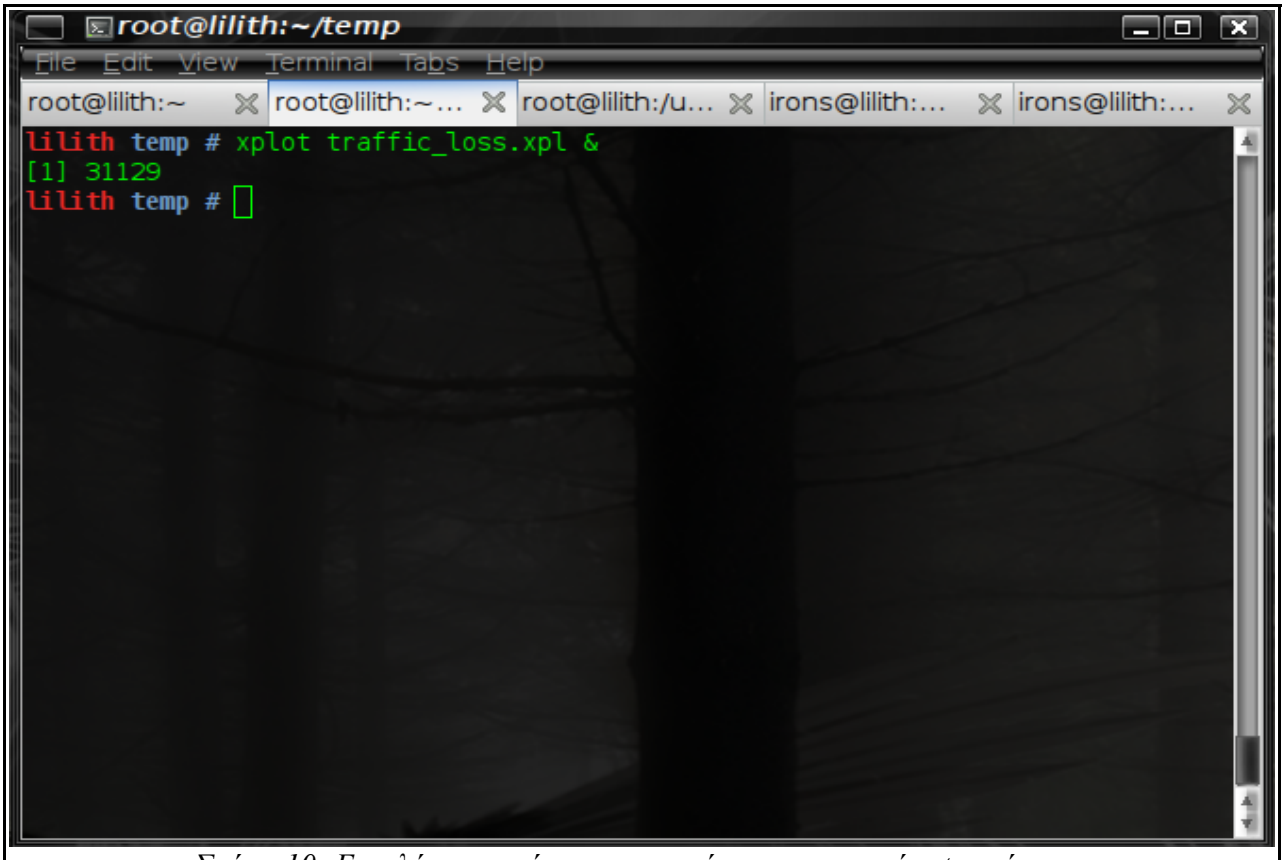
- Η κόκκινη γραμμή αντιπροσωπεύει το μέγιστο rtt που παρατηρήθηκε στο διάστημα μεταξύ δύο δειγματοληψιών.
- Η μπλέ γραμμή αντιπροσωπεύει το μέσο rtt που παρατηρήθηκε στο διάστημα μεταξύ δύο δειγματοληψιών.
- Η πράσινη γραμμή αντιπροσωπεύει το ελάχιστο rtt που παρατηρήθηκε στο διάστημα μεταξύ δύο δειγματοληψιών.

Γραφική Επανεκπομπών TCP Κίνησης

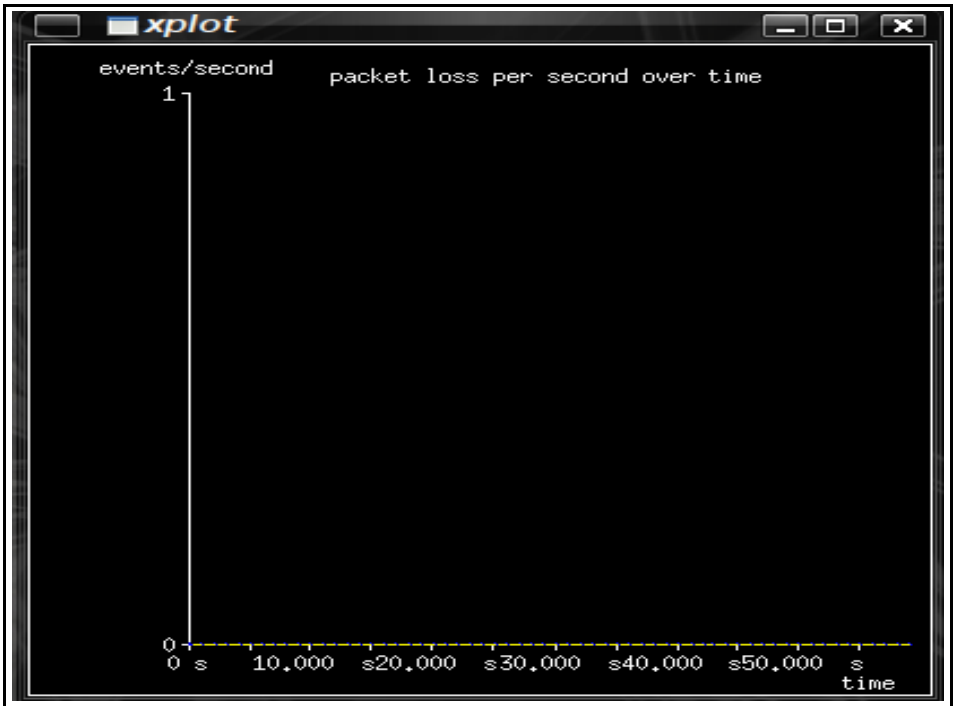
Εντολή: **tcptrace -zxy -xtraffic'-L -i1' test,, όπου το -i καθορίζει το χρόνο δειγματοληψίας.**



Σχήμα 9: Εντολή για δημιουργία γραφικής επανεκπομπών tcp κίνησης



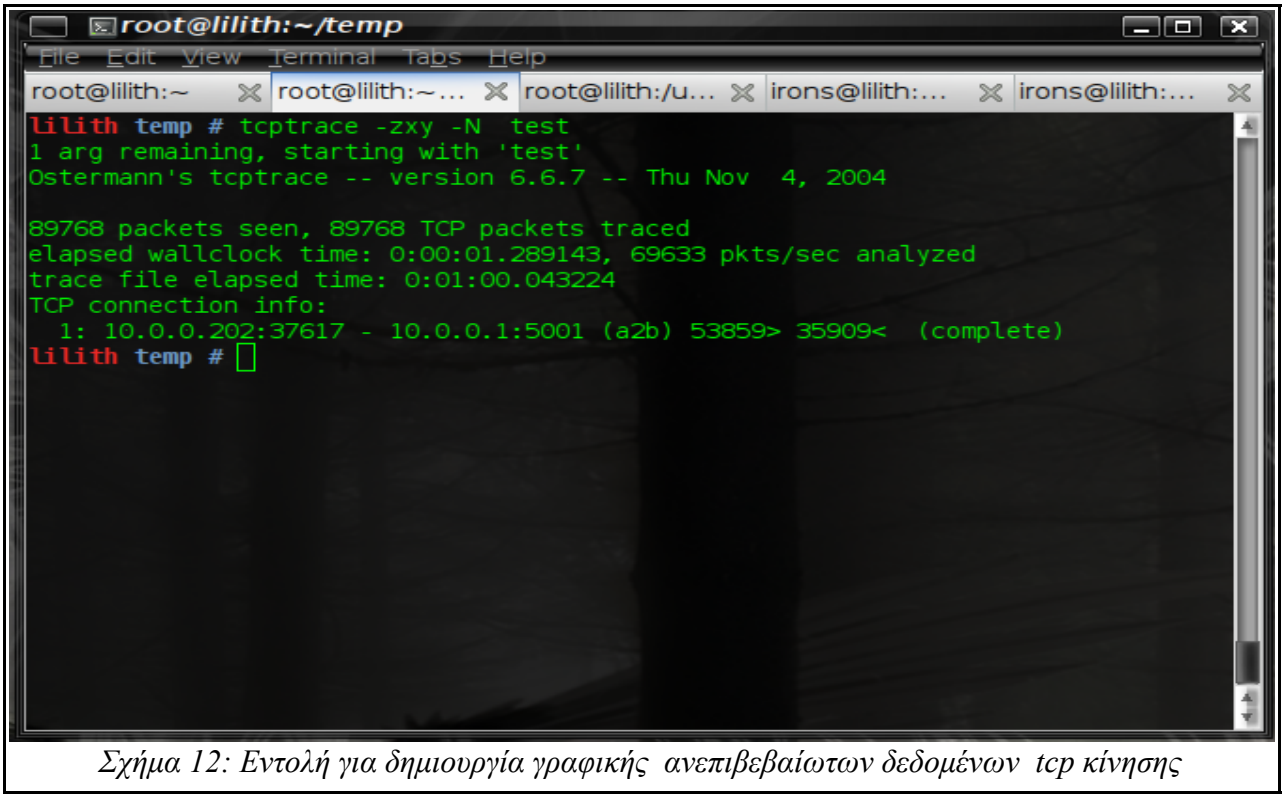
Σχήμα 10: Εντολή για εμφάνιση γραφικής επανεκπομπών tcp κίνησης



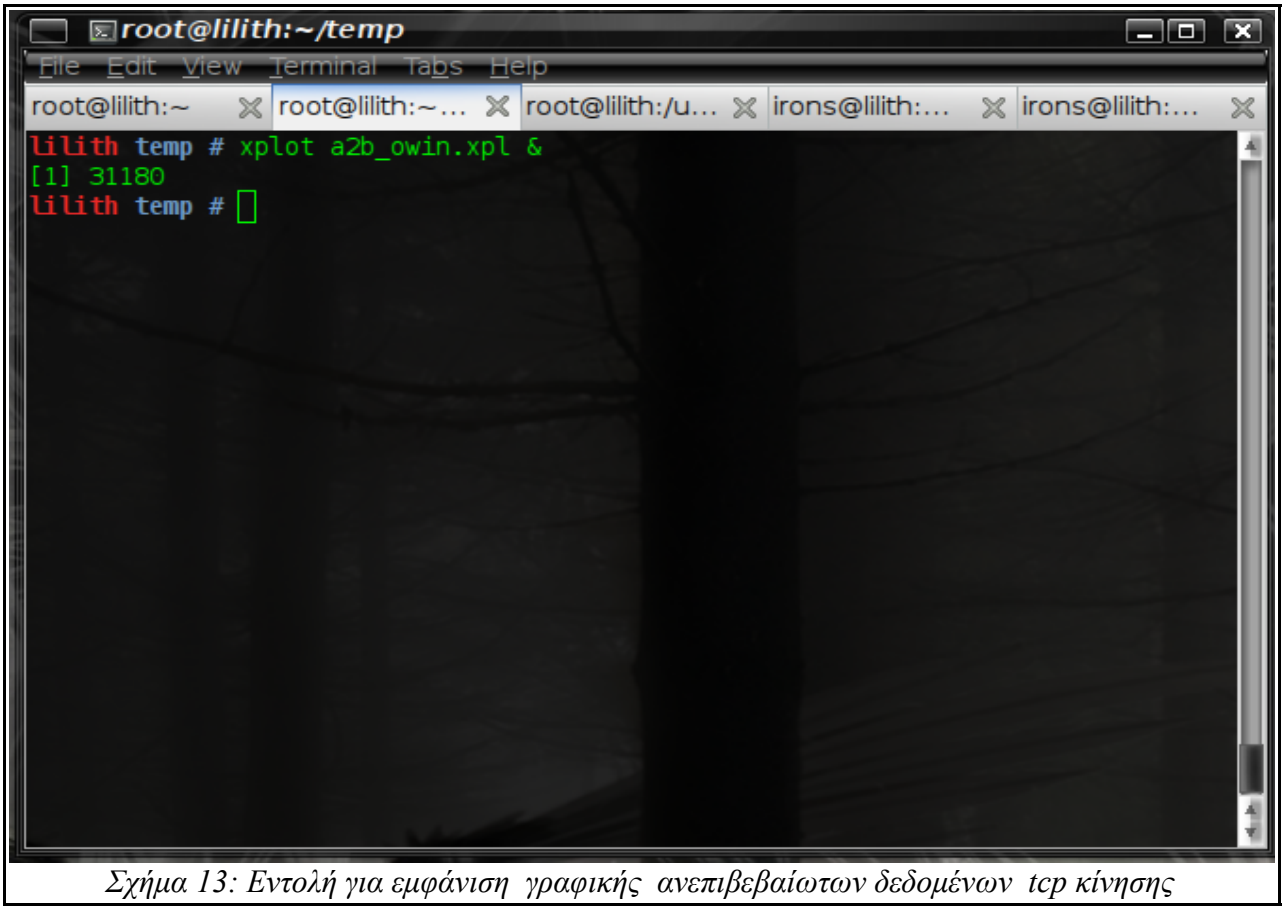
Σχήμα 11: Γραφική επανεκπομπών tcp κίνησης

Γραφική Ανεπιβεβαίωτων δεδομένων TCP Κίνησης

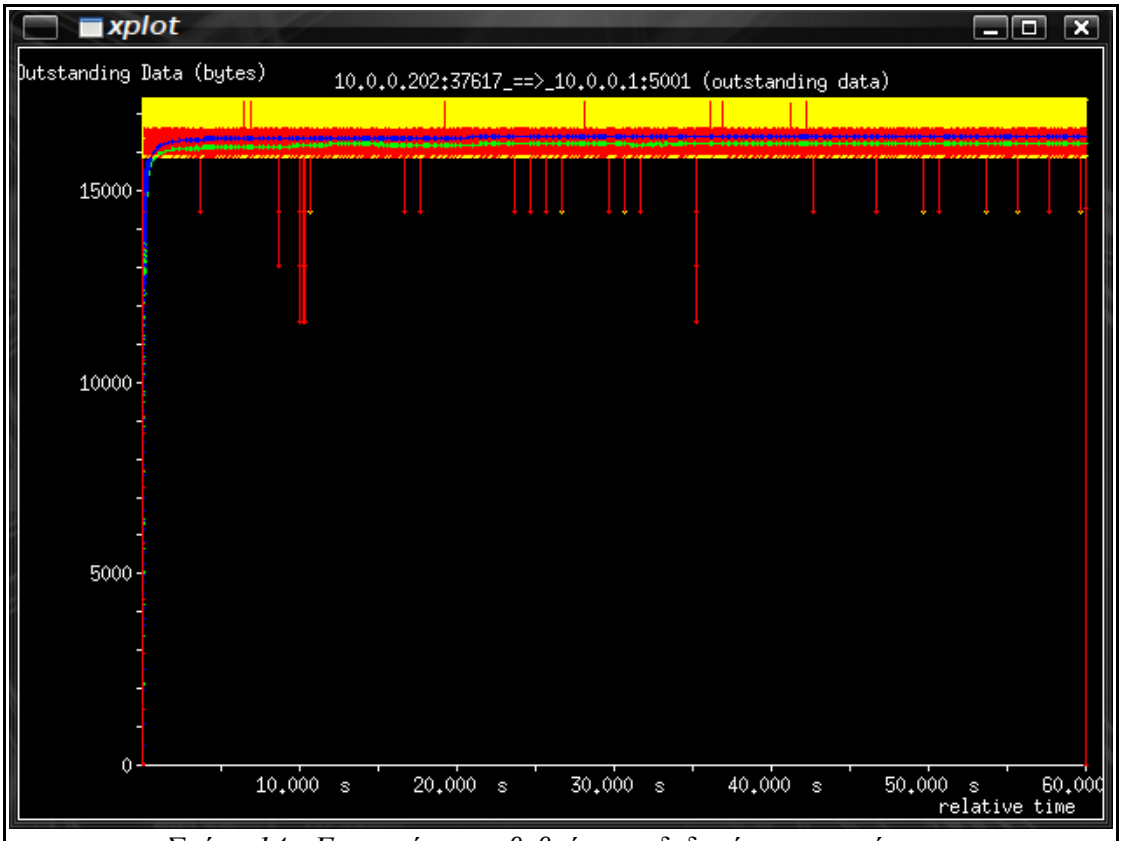
Εντολή: **tcptrace -zxy -N test**



Σχήμα 12: Εντολή για δημιουργία γραφικής ανεπιβεβαίωτων δεδομένων tcp κίνησης



Σχήμα 13: Εντολή για εμφάνιση γραφικής ανεπιβεβαίωτων δεδομένων tcp κίνησης



Σχήμα 14: Γραφική ανεπιβεβαίωτων δεδομένων tcp κίνησης

- Η κόκκινη γραμμή αντιπροσωπεύει τη στιγμιαία ποσότητα ανεπιβεβαίωτων δεδομένων στη

διάρκεια της σύνδεσης.

- Η μπλέ γραμμή αντιπροσωπεύει το μέσο όρο ανεπιβεβαίωτων δεδομένων μέχρι εκείνη τι στιγμή.
- Η πράσινη γραμμή αντιπροσωπεύει το εξομαλυμένο μέσο όρο ανεπιβεβαίωτων δεδομένων μέχρι εκείνη τι στιγμή.
- Η κίτρινη γραμμή αντιπροσωπεύει το διαφημιζόμενο παράθυρο (window) του άλλου υπολογιστή.

ΑΝΑΦΟΡΕΣ

[1] http://www.tcptrace.org/manual/index.html, "TCPTRACE Manual", (τελευταία προσπέλαση 19/04/2010)