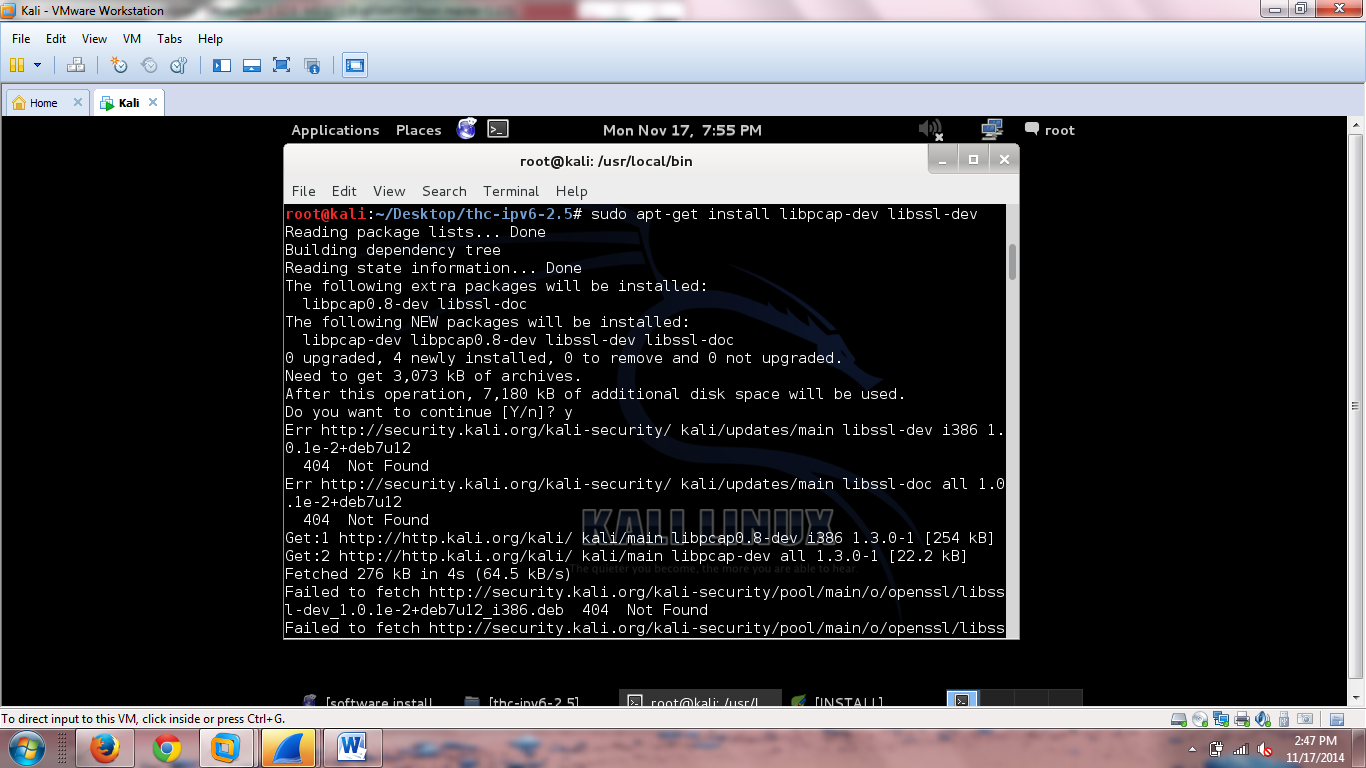
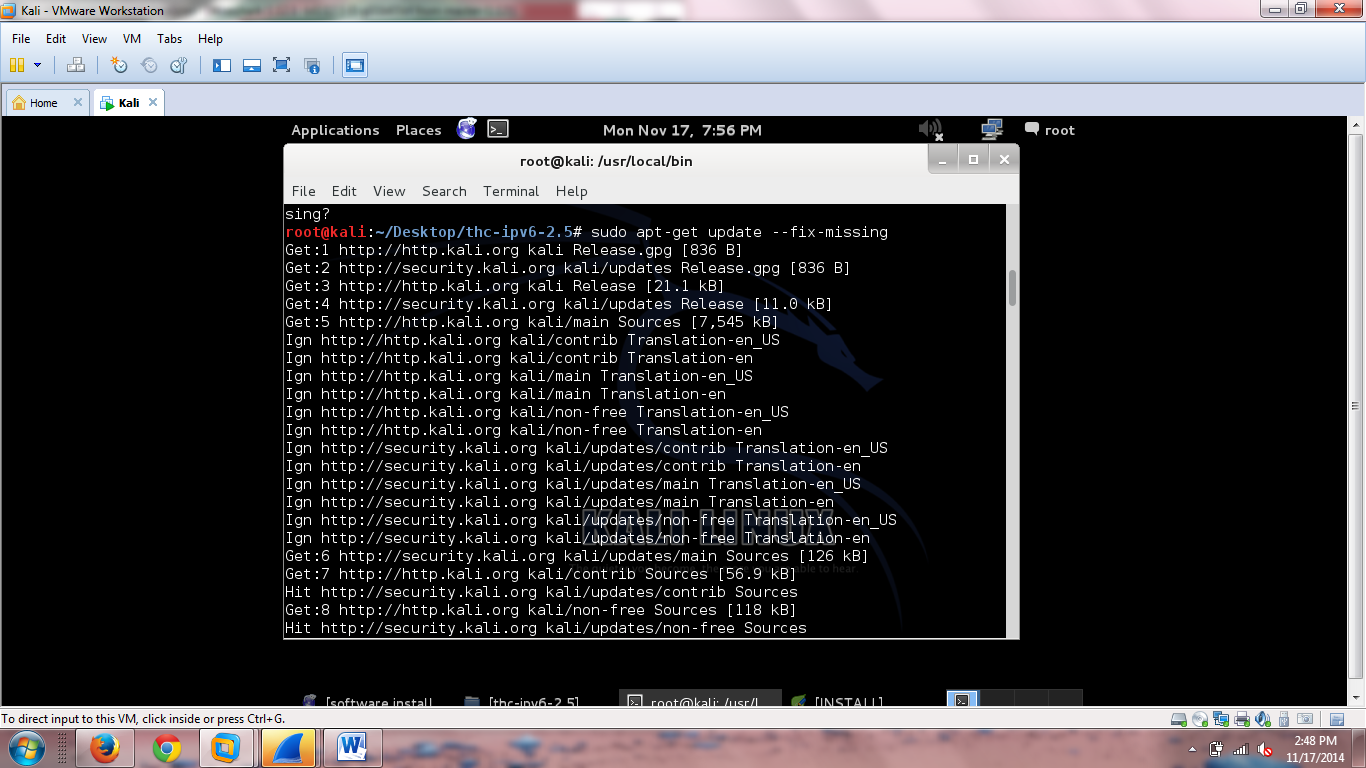
**Ryan Stearns  
CNA 432  
11/17/2014  
Lab 7**

**INSTALL**

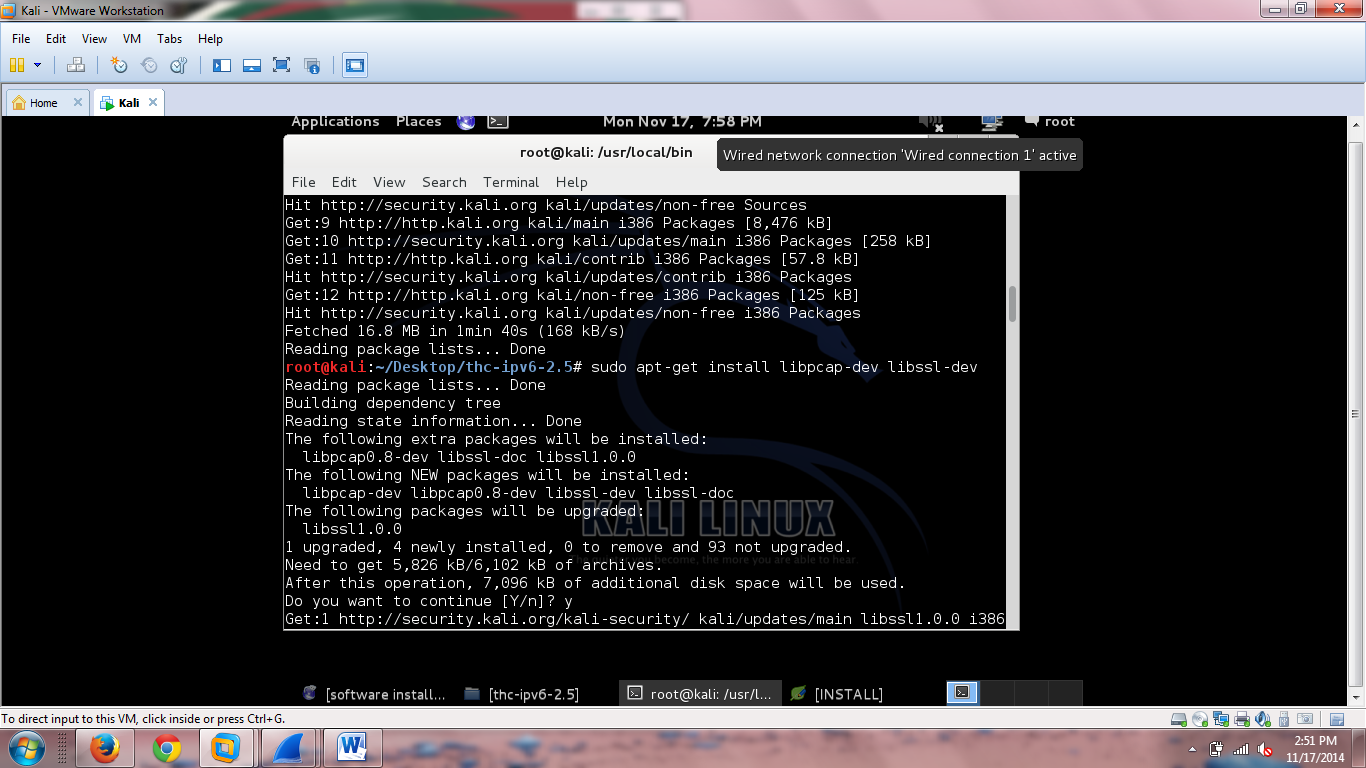
As per the INSTALL readme included in the thc-ipv6-2.5 package, first I had to install libpcap and libssl.



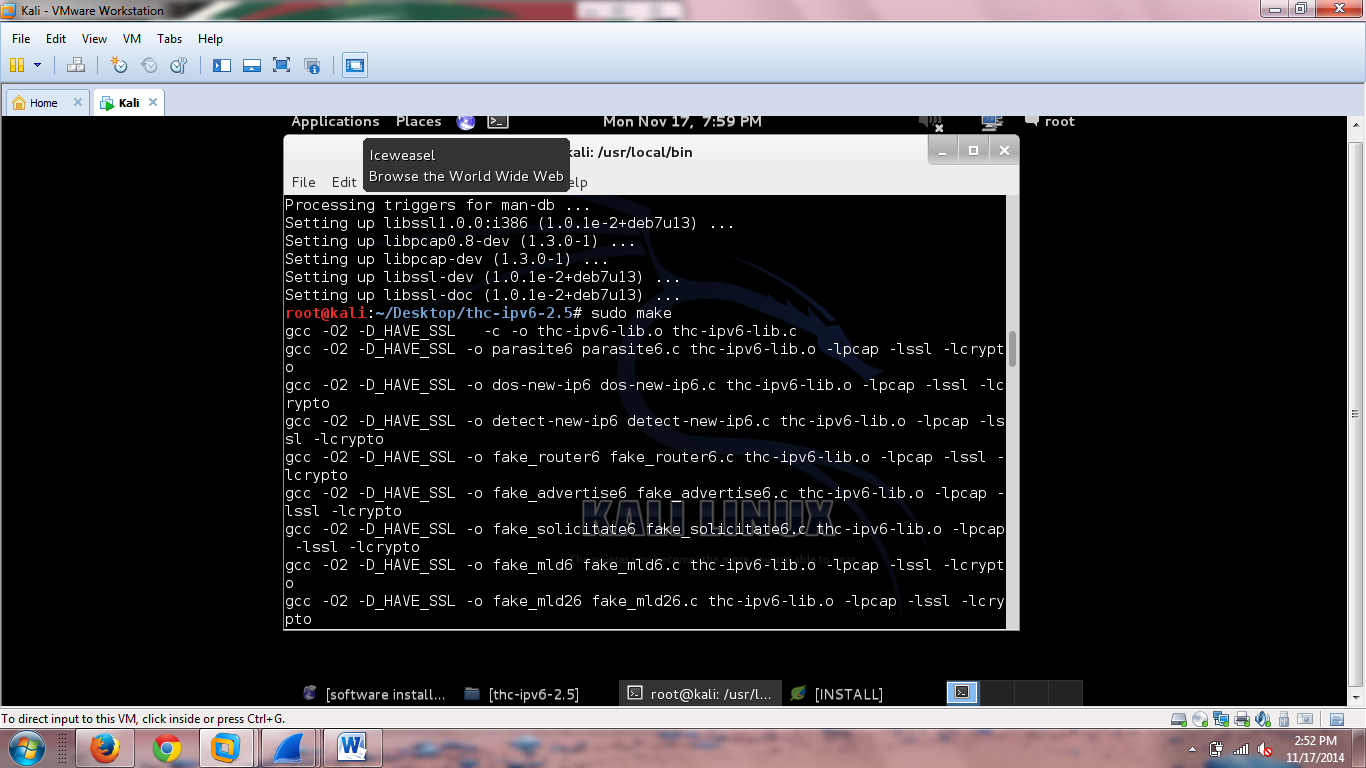
This was unsuccessful, so I had to fix missing files to try to fix the errors I was receiving.



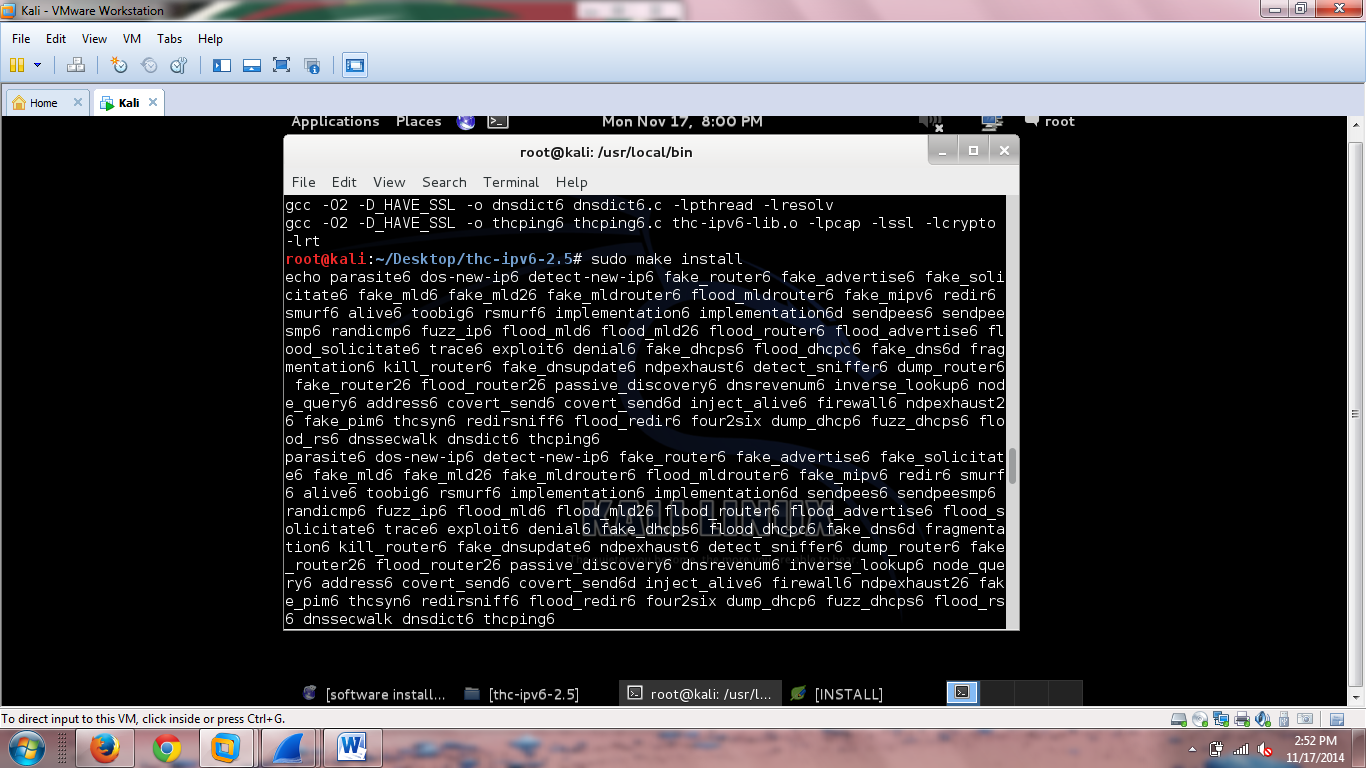
After the –fix-missing update was applied, I reinstalled libpcap and libssl.



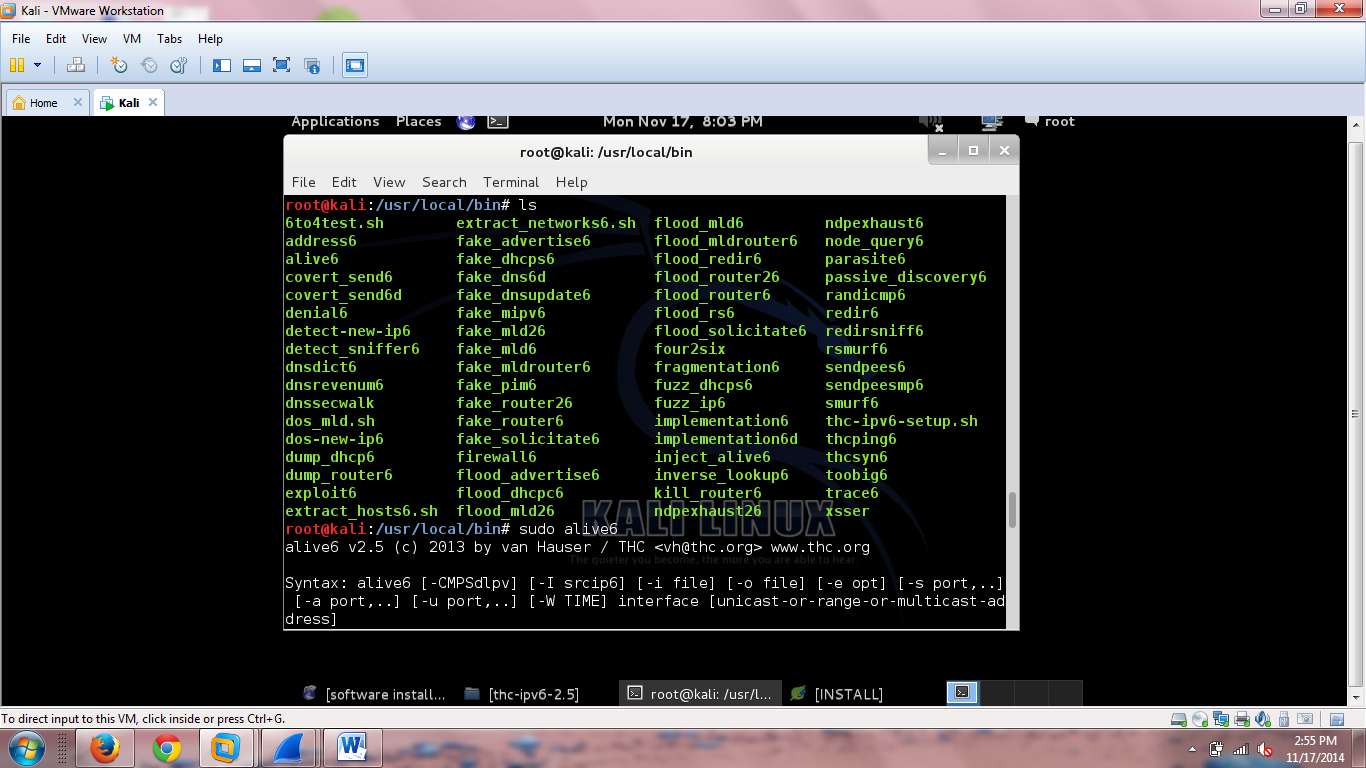
After that was successful, I executed the “sudo make” command



After the make command, I executed the “sudo make install” command

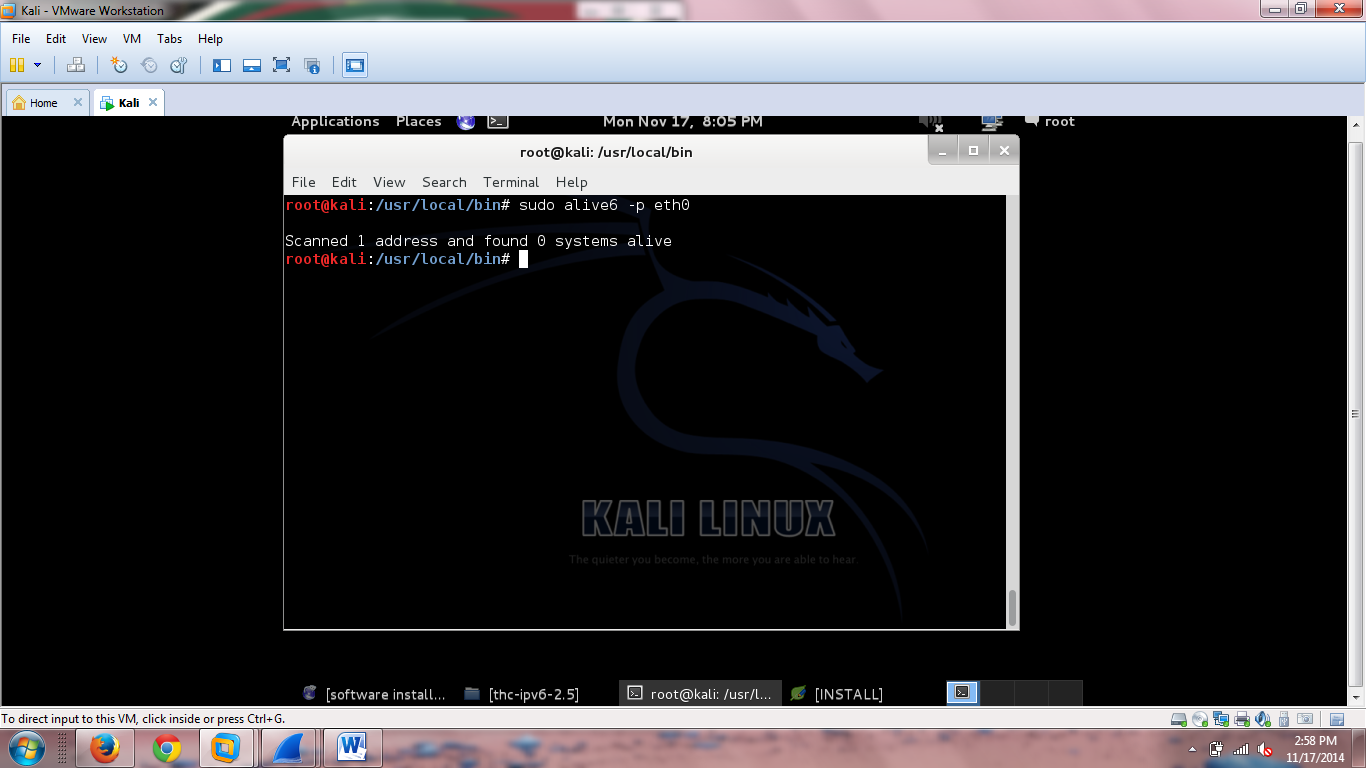


Most of the tools were installed to /usr/local/bin



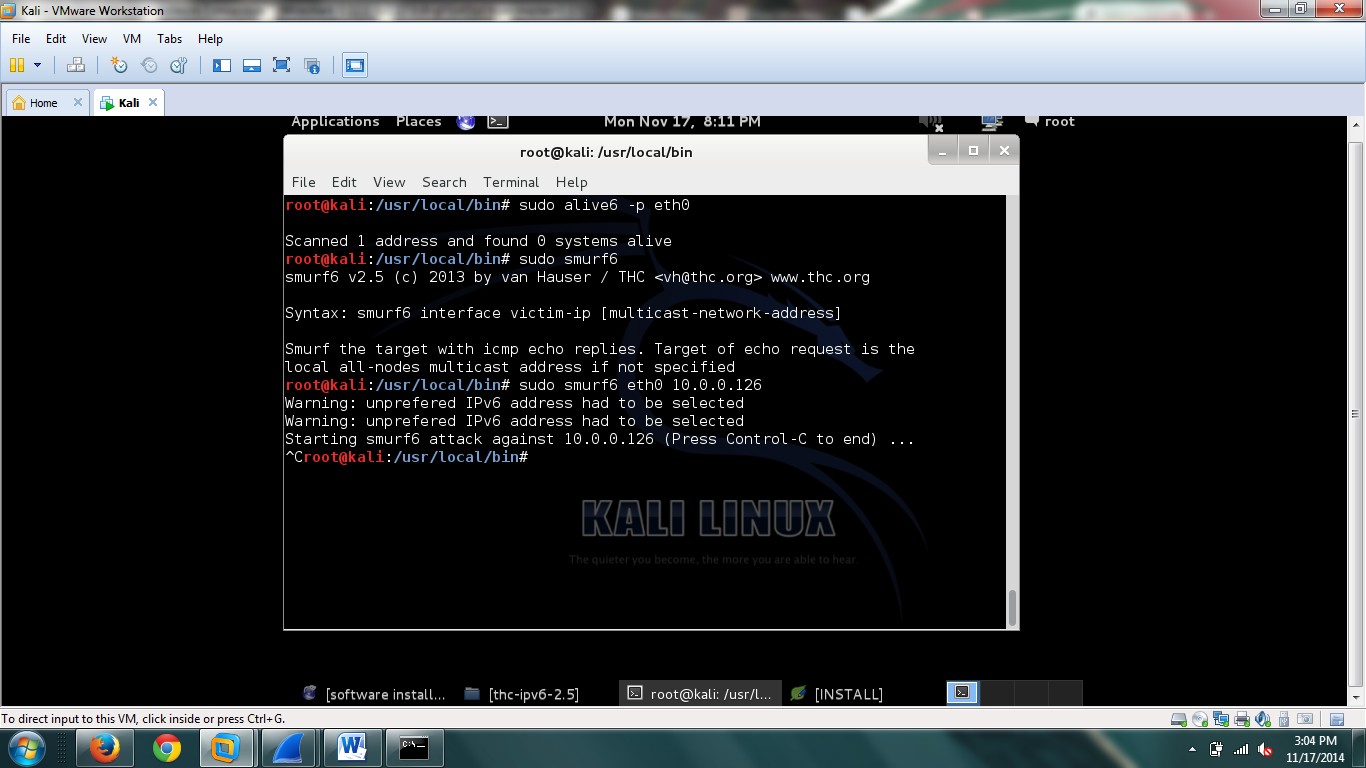
**ALIVE6**

Below is the output of the alive6 command, not ran on an IPV6 network.

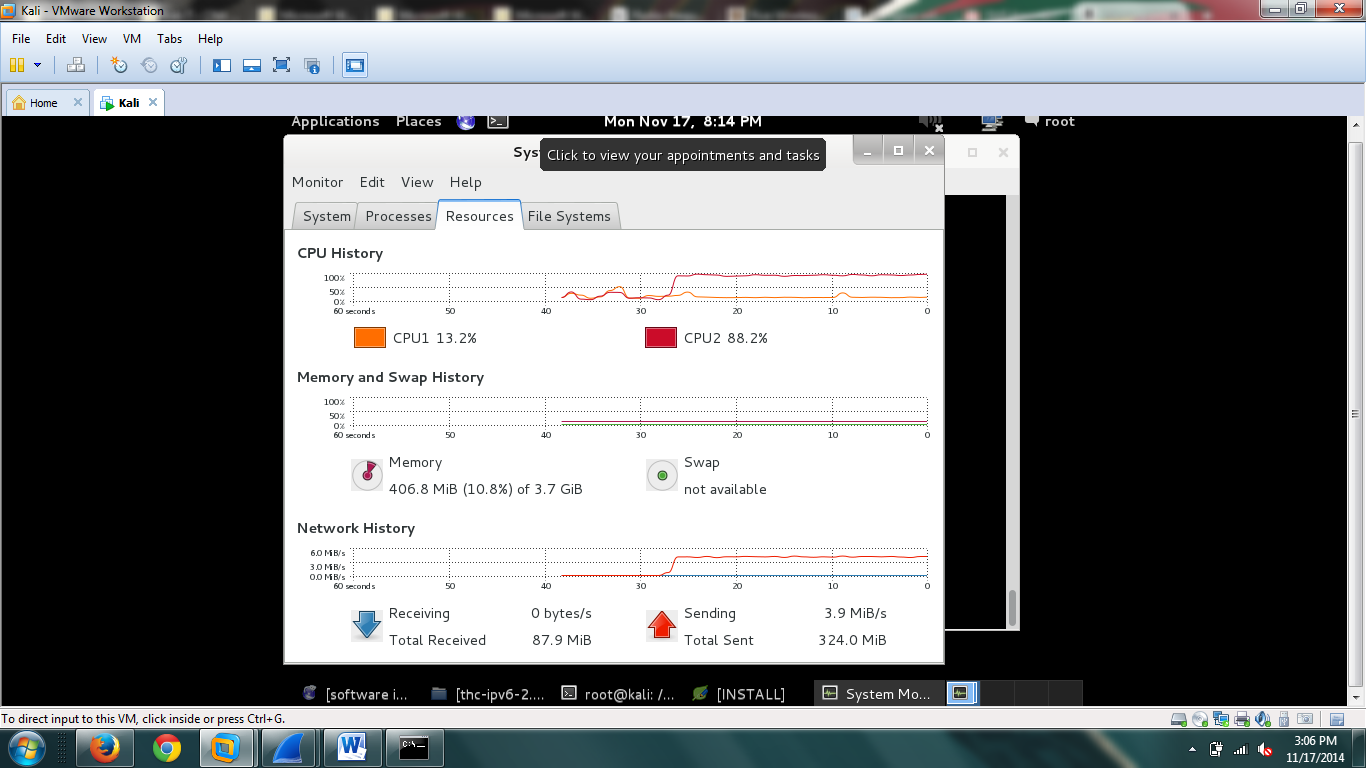


**SMURF6**

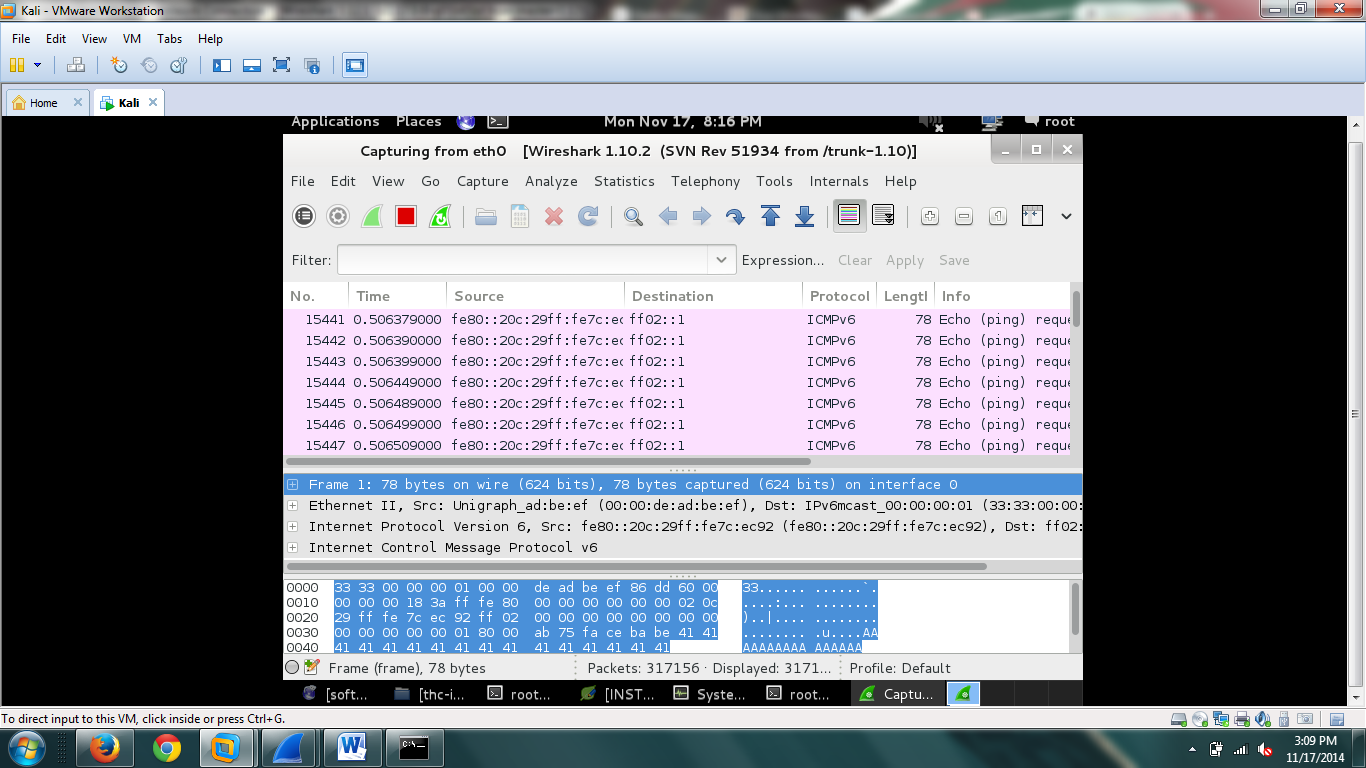
Below is the output of the smur6 command, also not ran on an IPV6 network



Below is the resource monitor. There is a large spike in the CPU Graph, as well as the Network History graph when Smurf6 is executed.

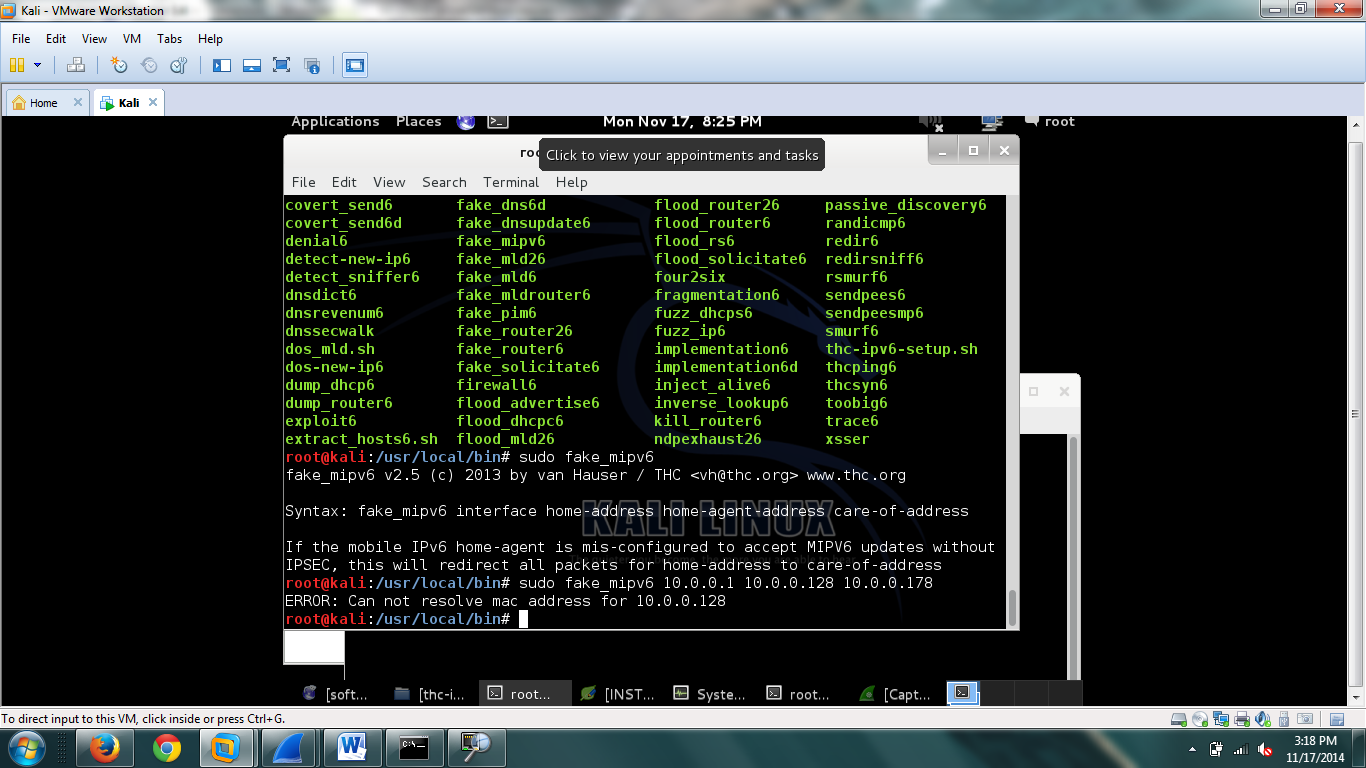


Below is the ICMPv6 Traffic generated by Smurf6



**Fake\_mipv6**

Below is fake\_mipv6, also not ran on an IPV6 network.



**Alive6**

Alive6 “shows alive addresses in the segment. If you specify a remote router, the packets are sent with a routing header prefixed by fragmentation.” [2]

**Smurf6**

Smurf6 can be used to overwhelm a host by generating a plethora of ICMP traffic. Not only does this put a heavy load onto the host, it also has a high overhead of the machine running the Smurf6 Command, as seen in the resource monitor screen shot. The Smurf6 command can be useful for Network Stress Testing, but can also be manipulated to overwhelm a network host.

**Fake\_MIPv6**

MIPv6 has a lot of vulnerabilities that could potentially be exploited. “It is possible to create routing loops among HAs. This is achieved when a MN binds its HoA located on the first HA to its second HoA located on the second HA. Such a type of binding force the two Has to tunnel and re-tunnel data packets while re-routing them between themselves without knowledge that a routing loop has been created.” [1]

**Resources**

[1] Draft-Haddad-Mext-Mip6-Residual-Threats-02, and Ietf 72 July 200. *Mobile IPv6 Residual Threats* (n.d.): n. pag. *MIP6\_Research*. Web.  
 <http://www.ietf.org/proceedings/72/slides/mext-3.pdf>

[2] "THC-IPv6-Attack-Toolkit/alive6." *- Aldeid*. N.p., n.d. Web. 17 Nov. 2014.  
 <http://www.aldeid.com/wiki/THC-IPv6-Attack-Toolkit/alive6>