**Lab 14: Data Encoding**

**Course Name:** Malware Analysis and Reverse Engineering (IAM302)

**Student Name:** Nguyễn Trần Vinh – SE160258

**Instructor Name:** Mai Hoàng Đỉnh

**Lab Due Date:** 29/2/2023

**Purpose**

You will practice the techniques in chapter 13

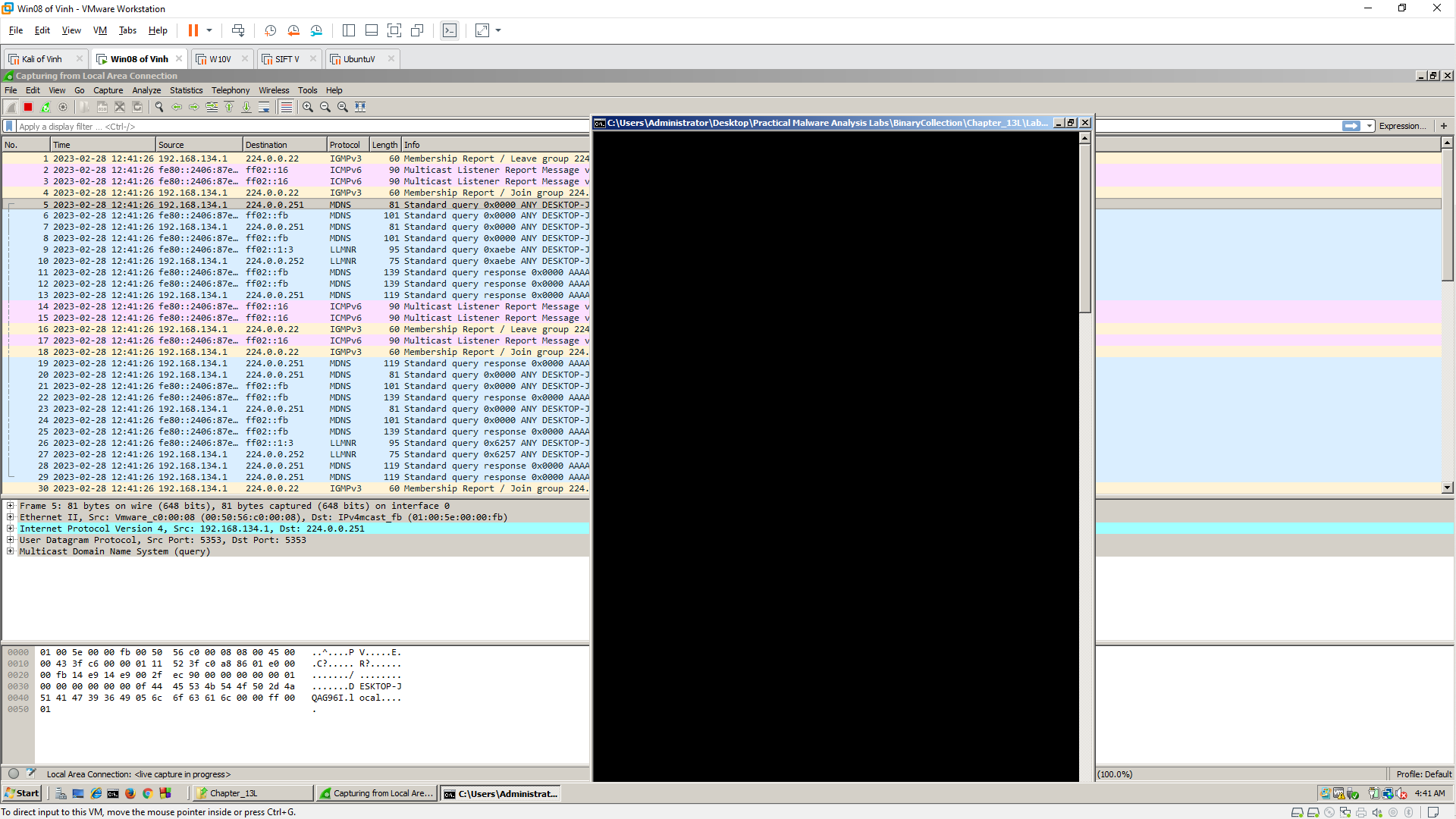
**What you need:**

* A Windows machine with the tools we have been using installed.

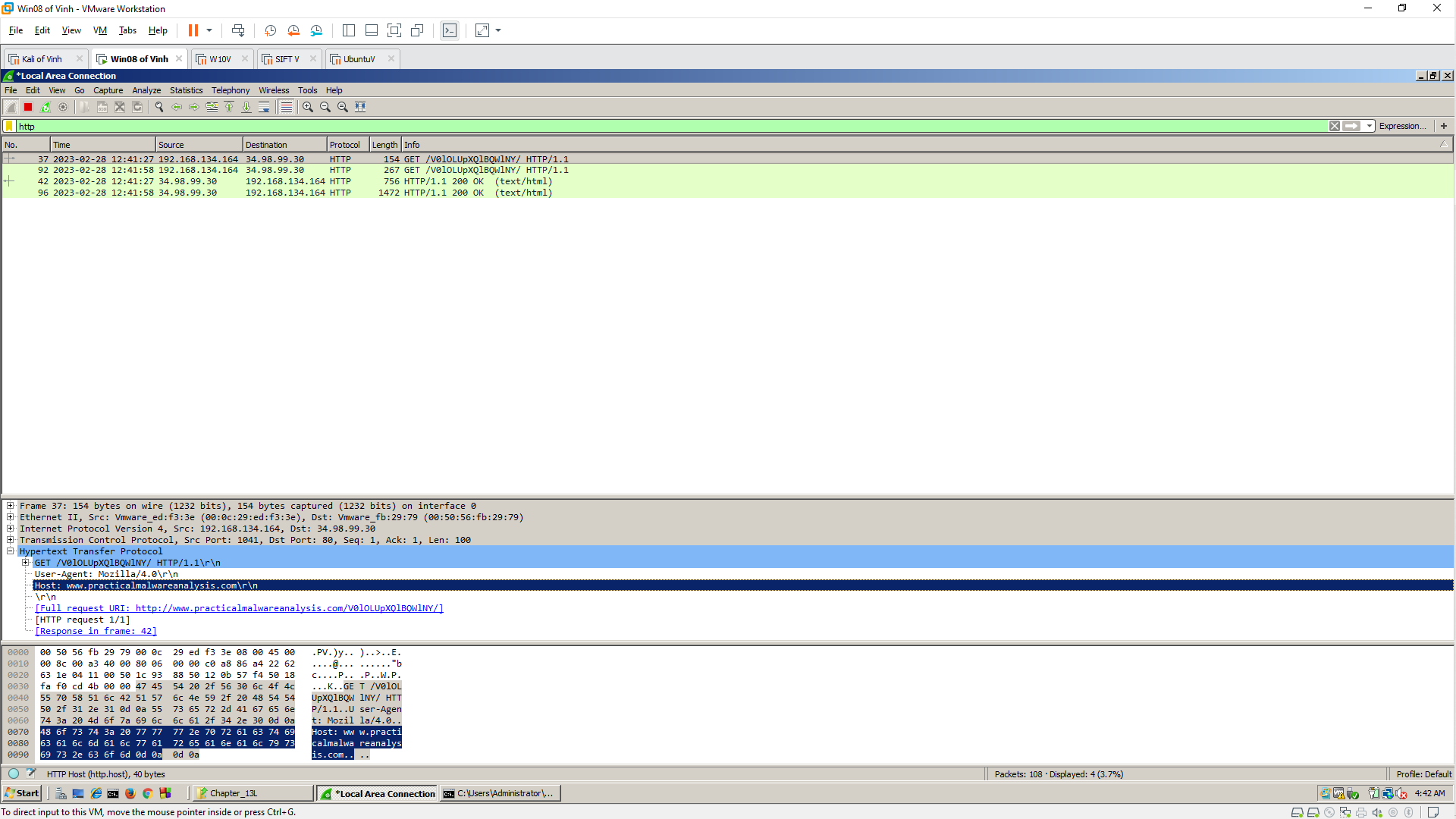
**Beacons**

* The book recommends running the malware with another VM simulating the Internet with inetsim, but I don't see any good reason to bother with that. I just connected a VM to the real Internet and ran the malware.

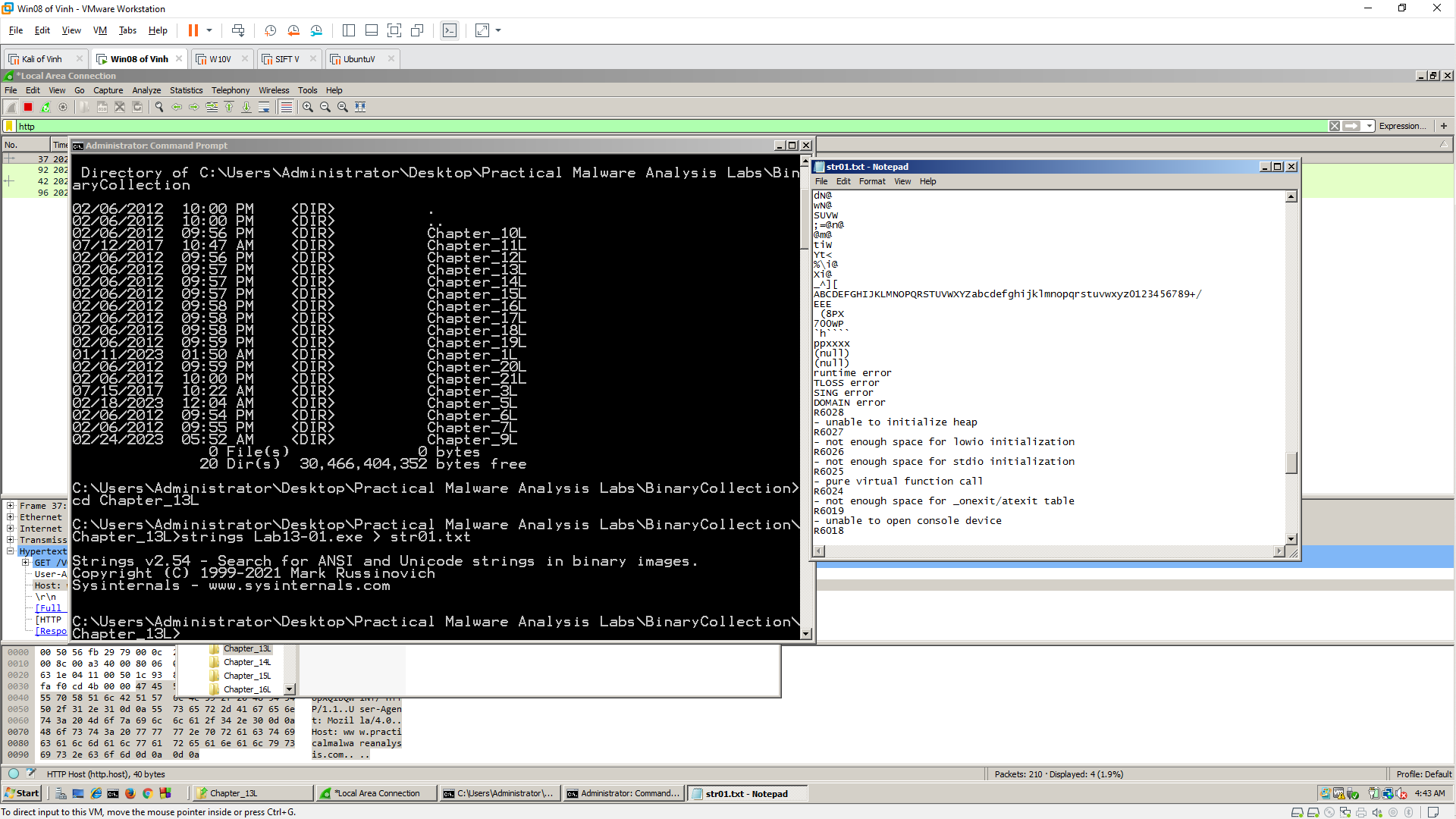
**Launch the Lab13-01.exe file**

****

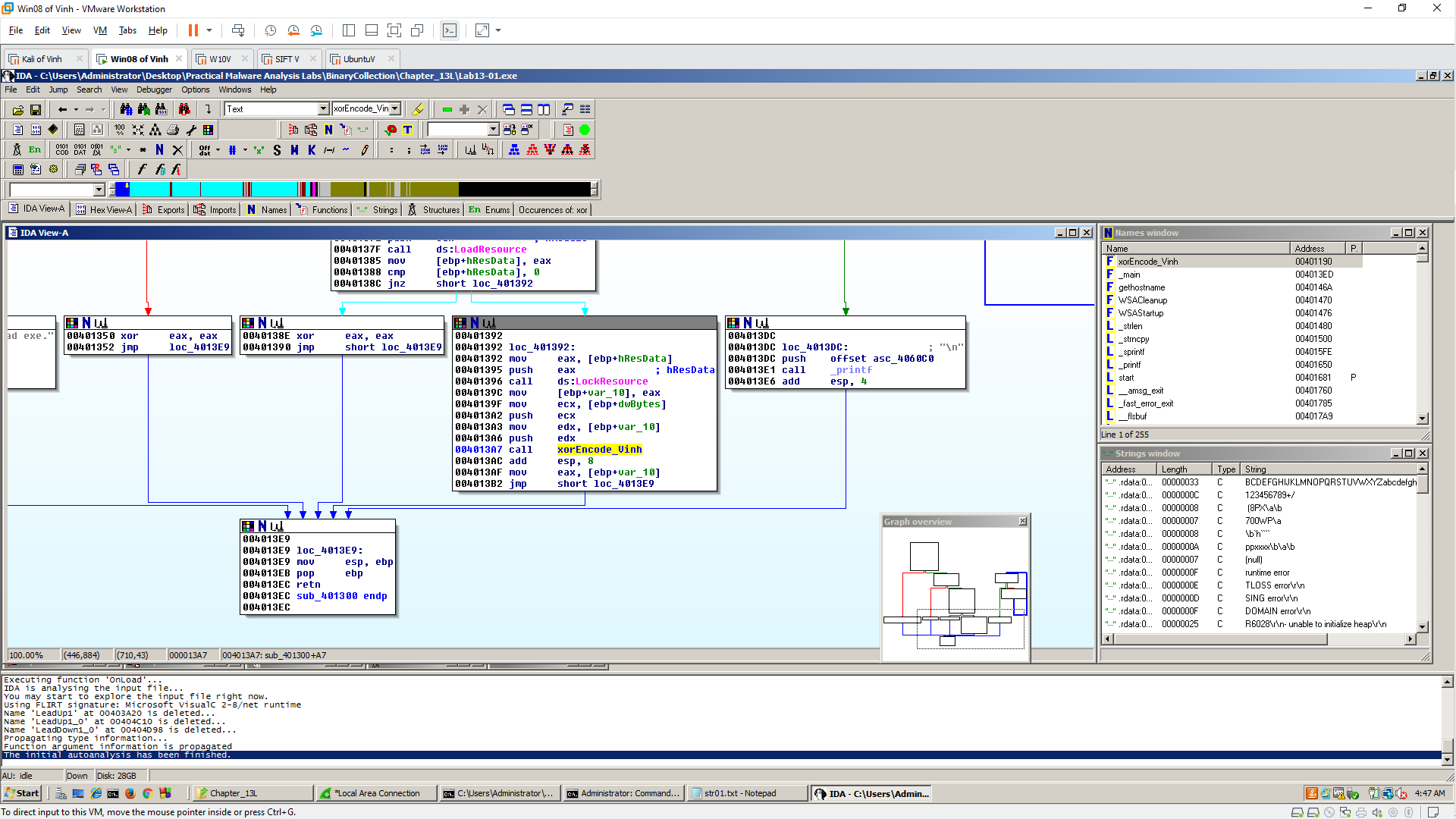
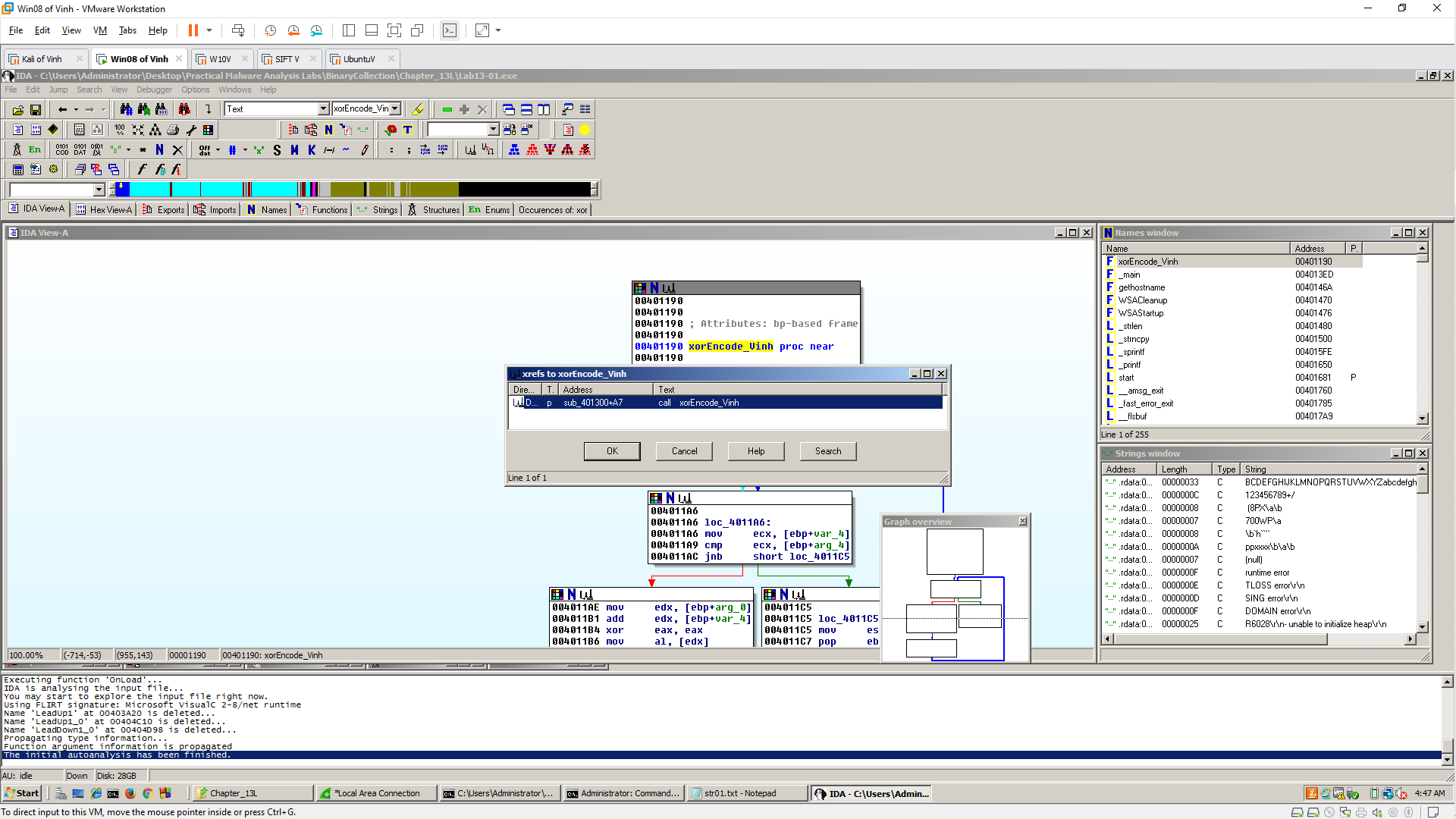
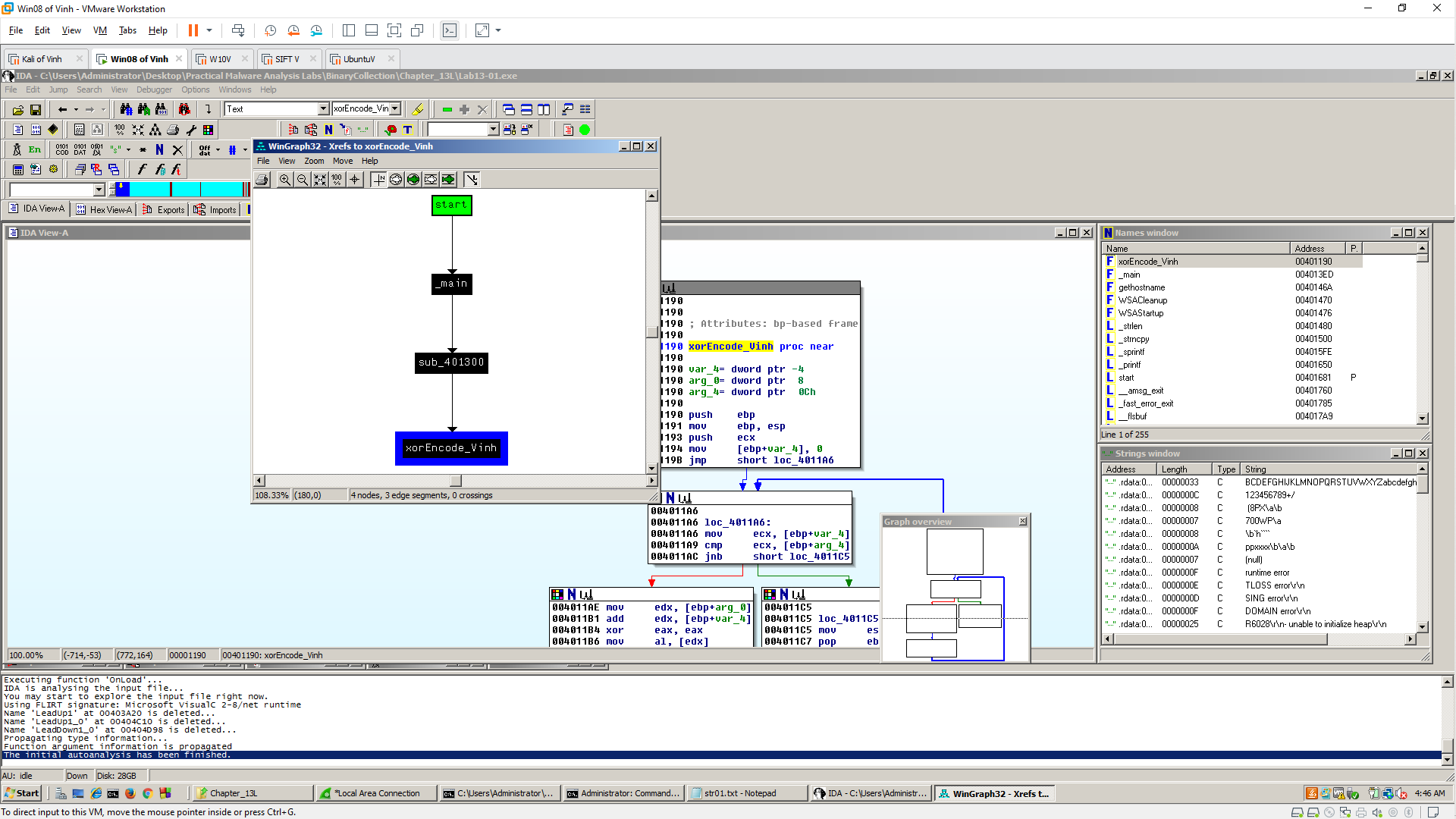
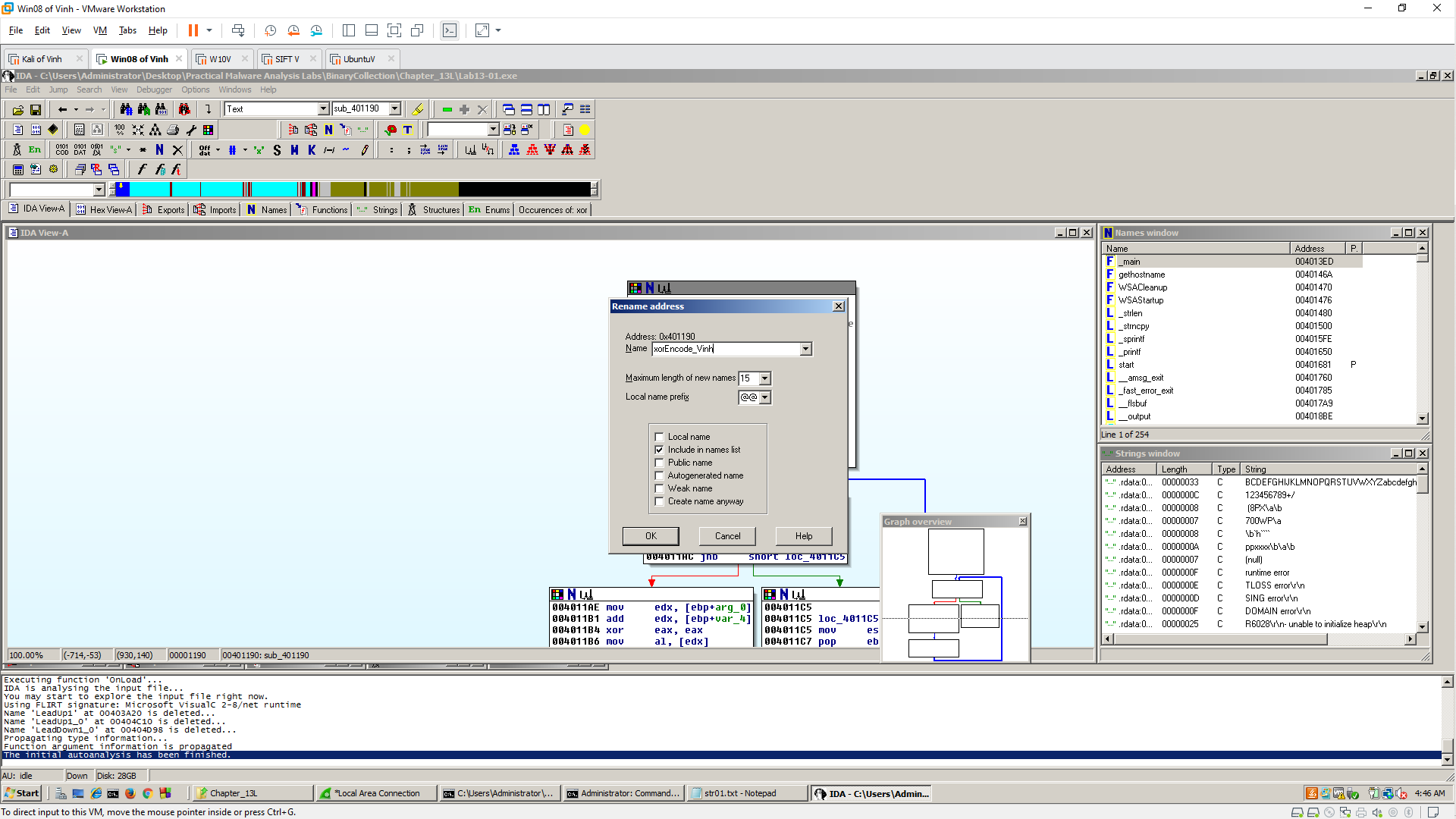
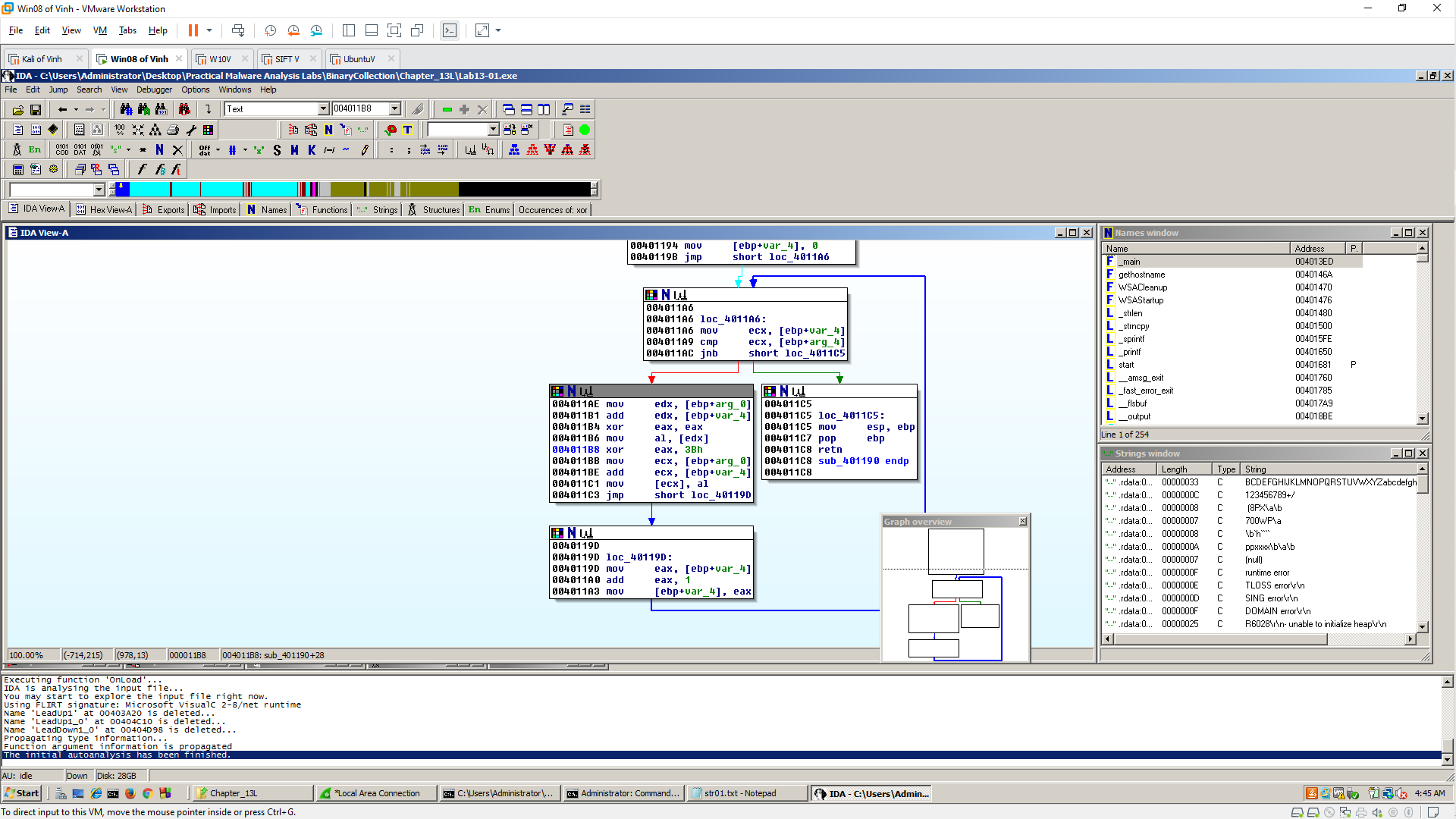
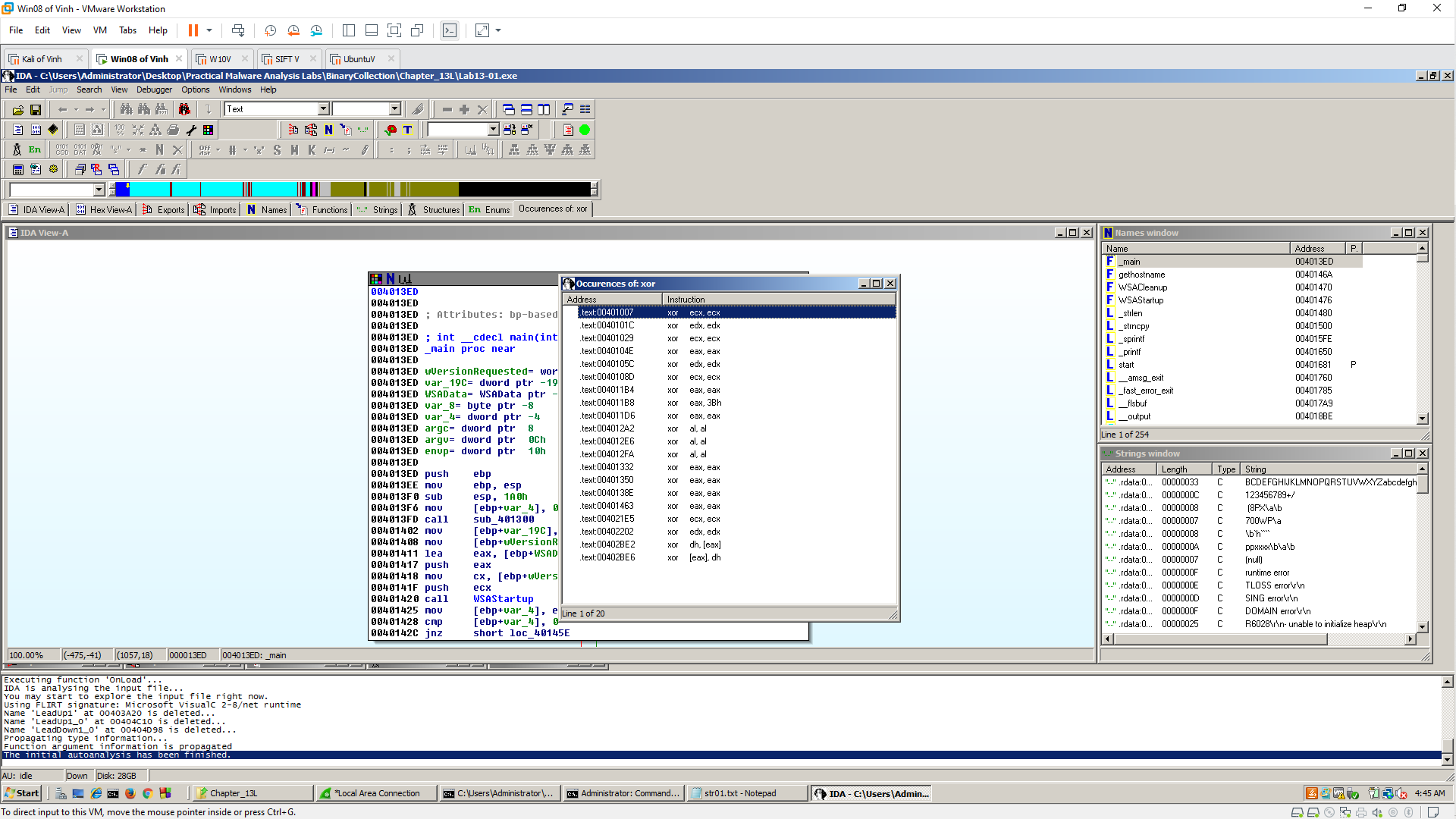
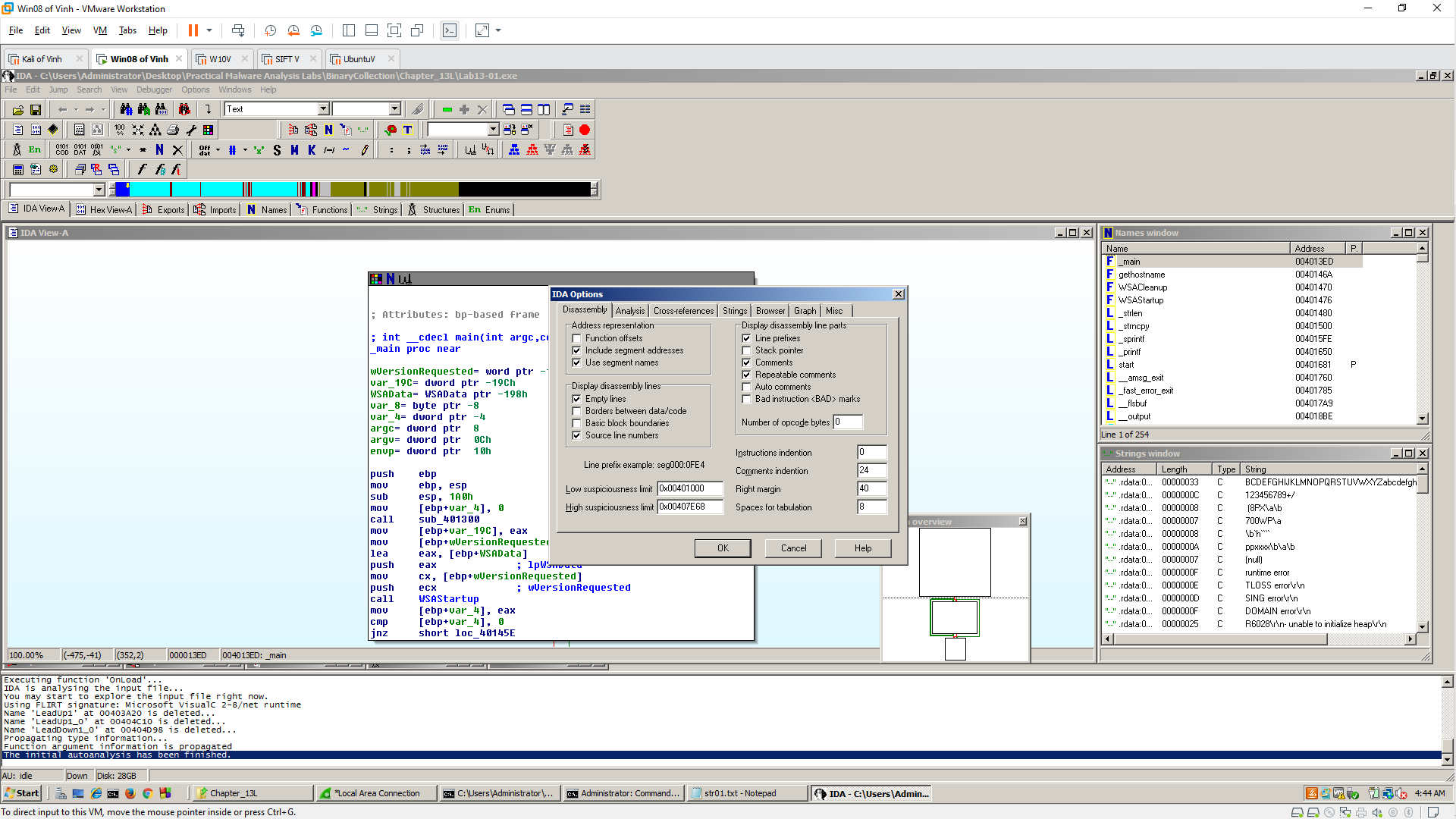
**Wireshark**

****

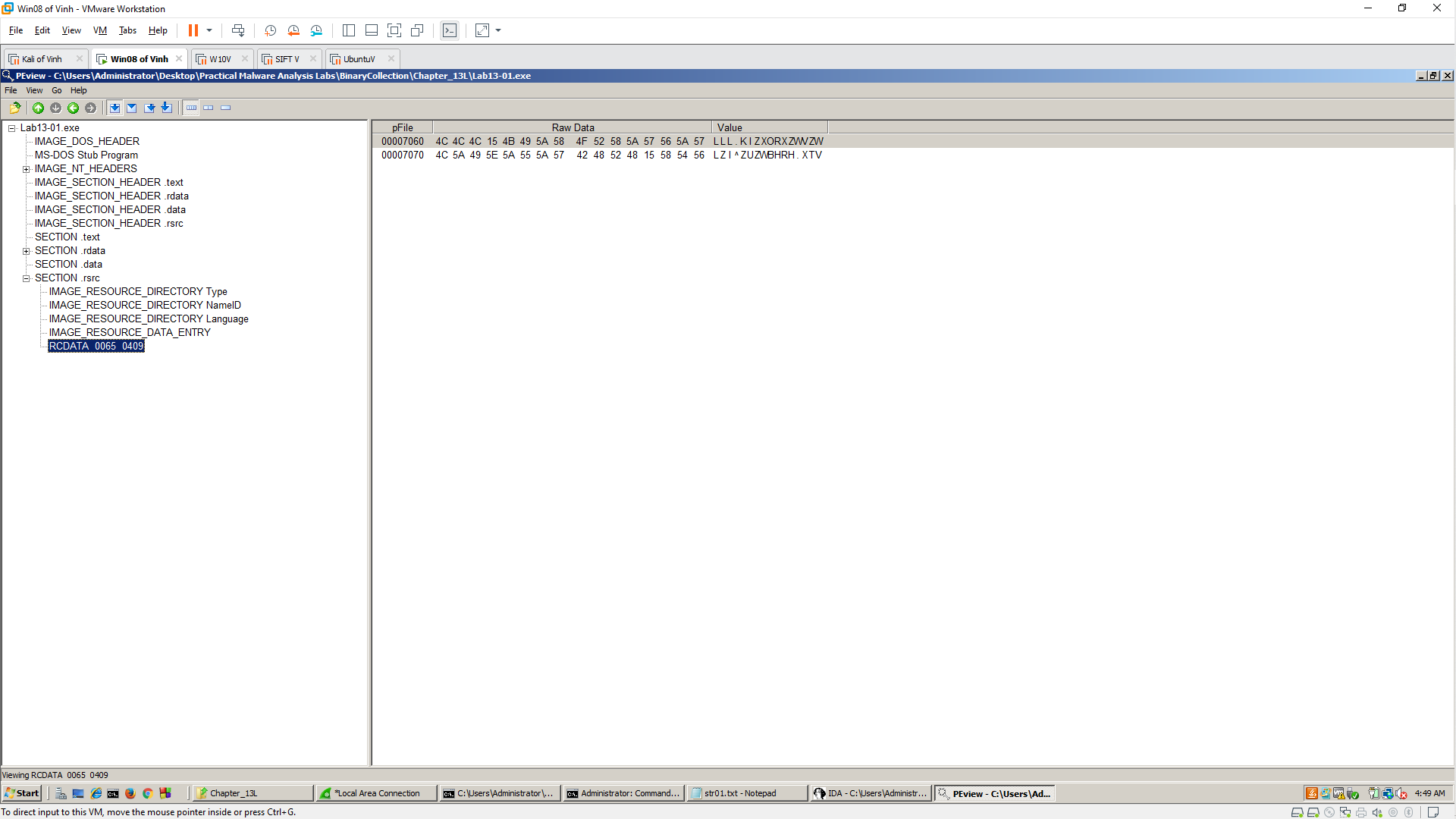
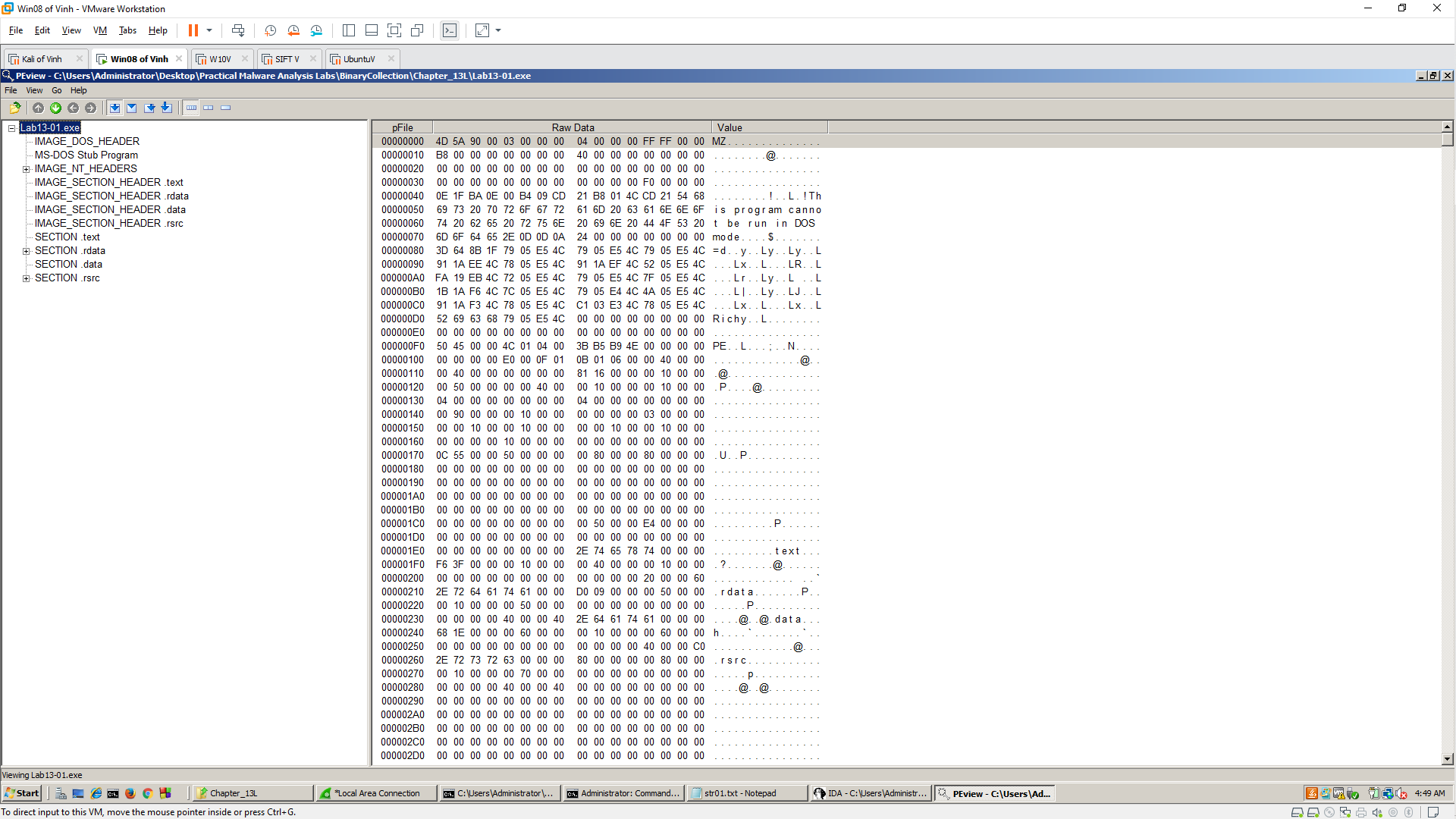
**Strings**

****

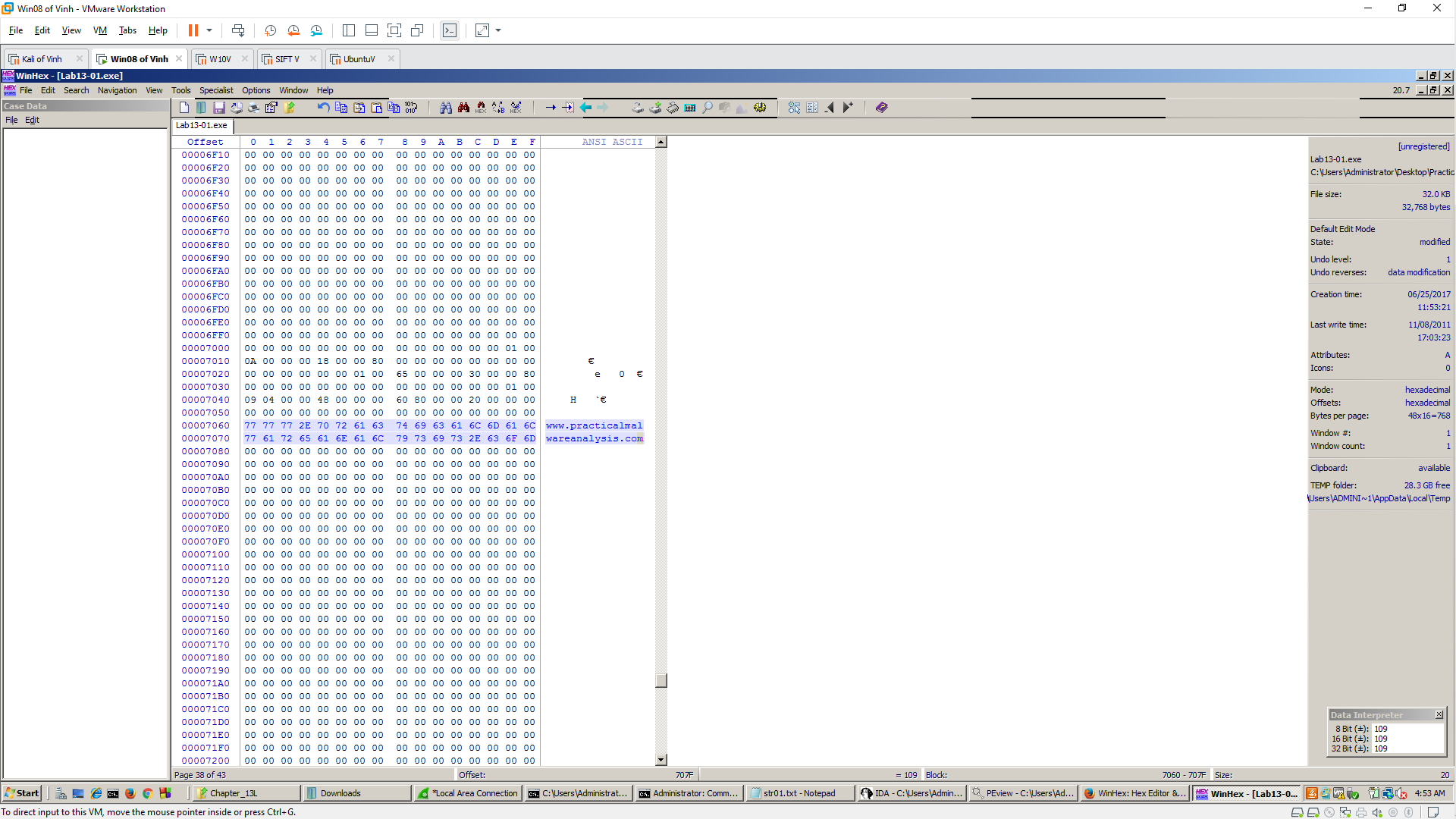
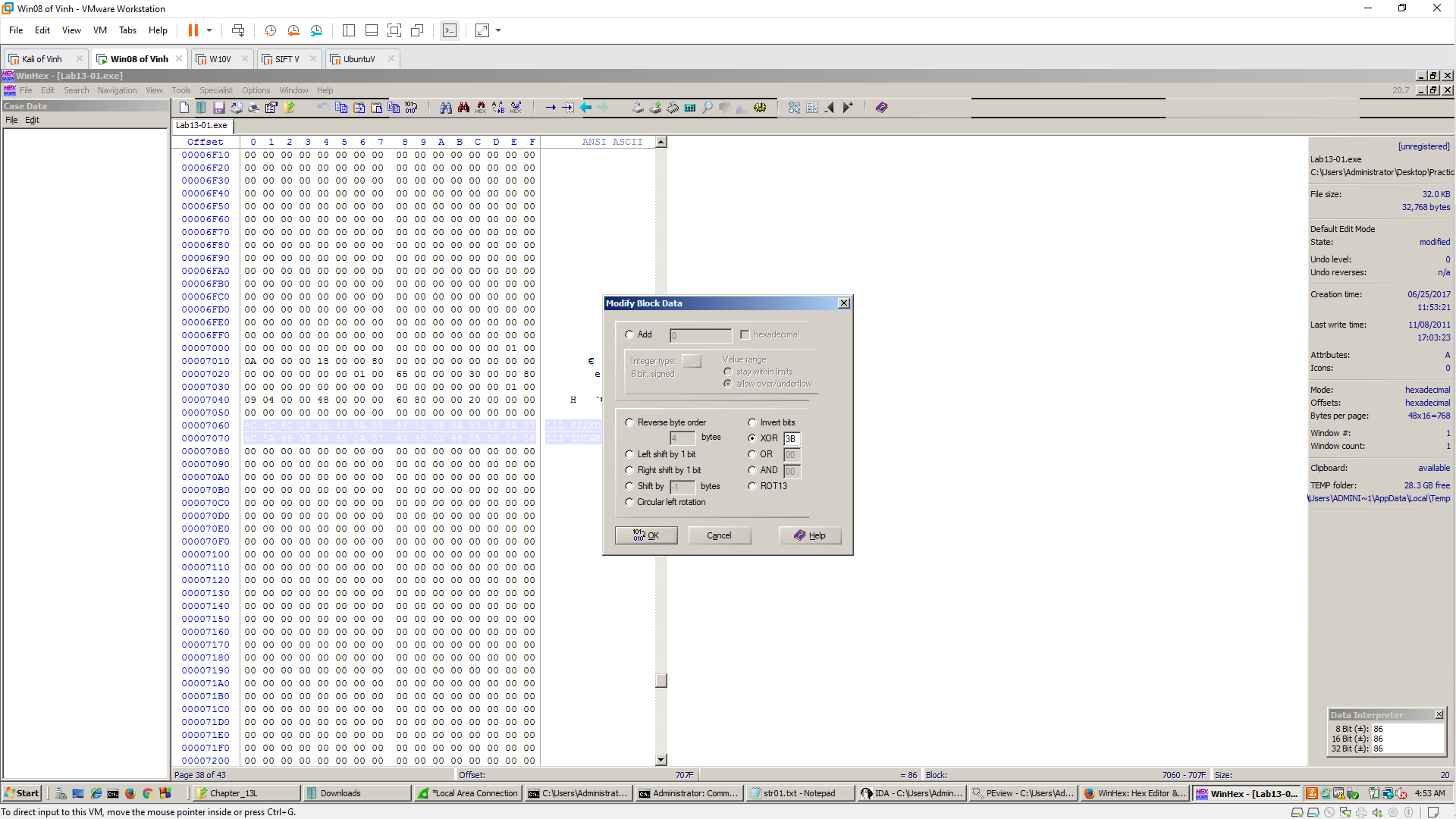
**IDA Pro**

****

**PEview**

****

**WinHex**

****