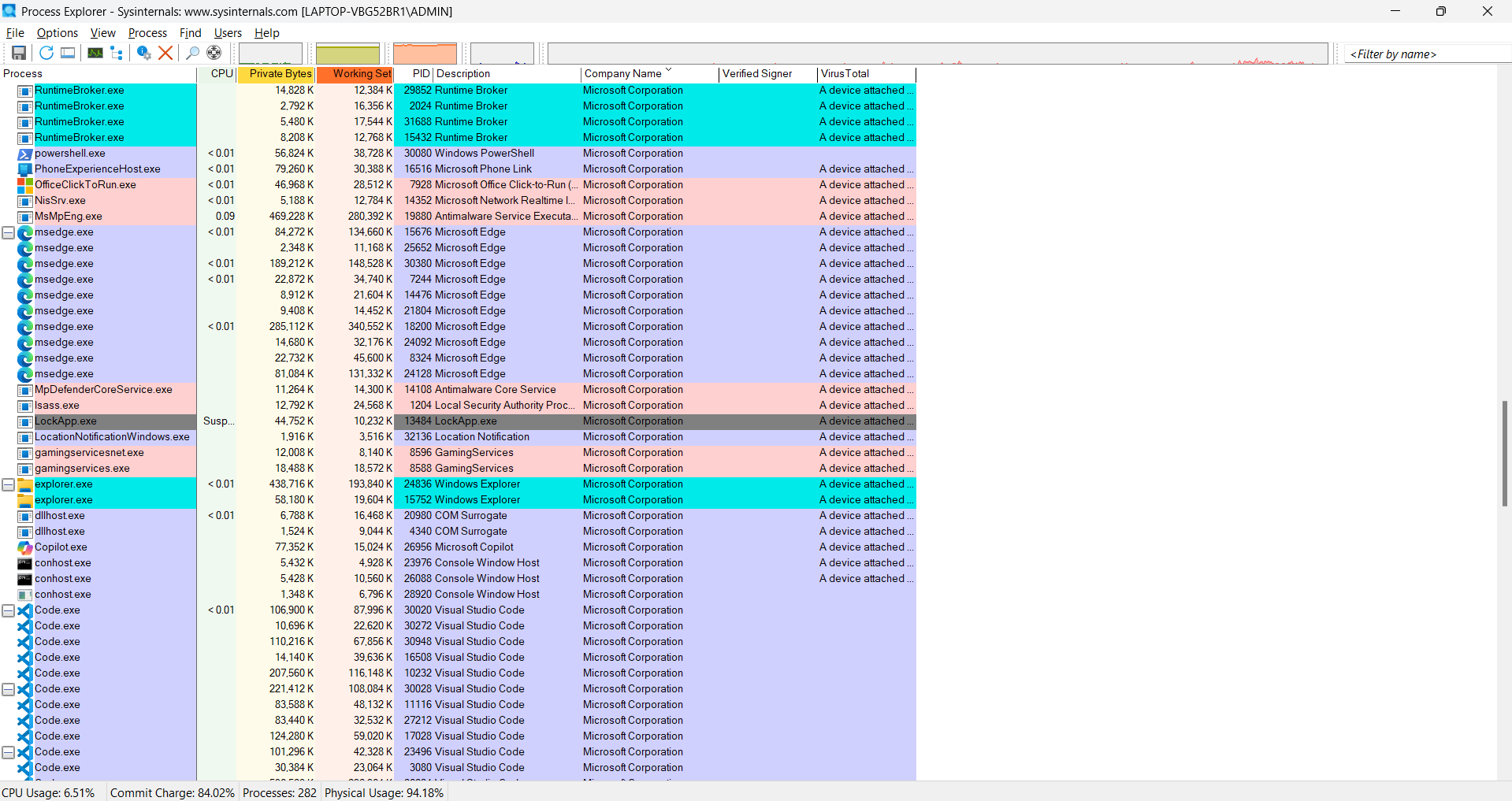
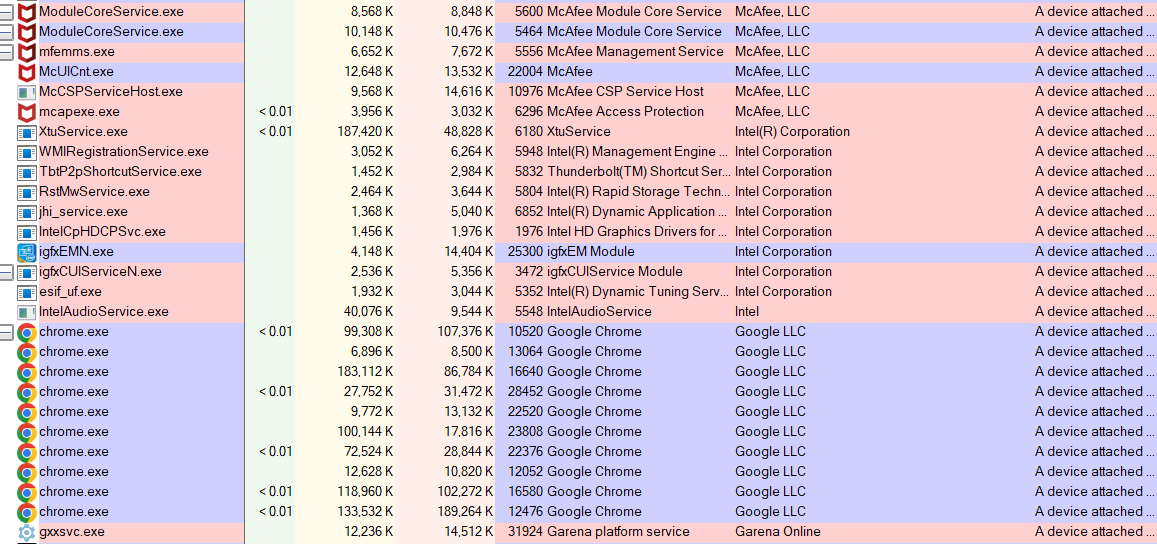
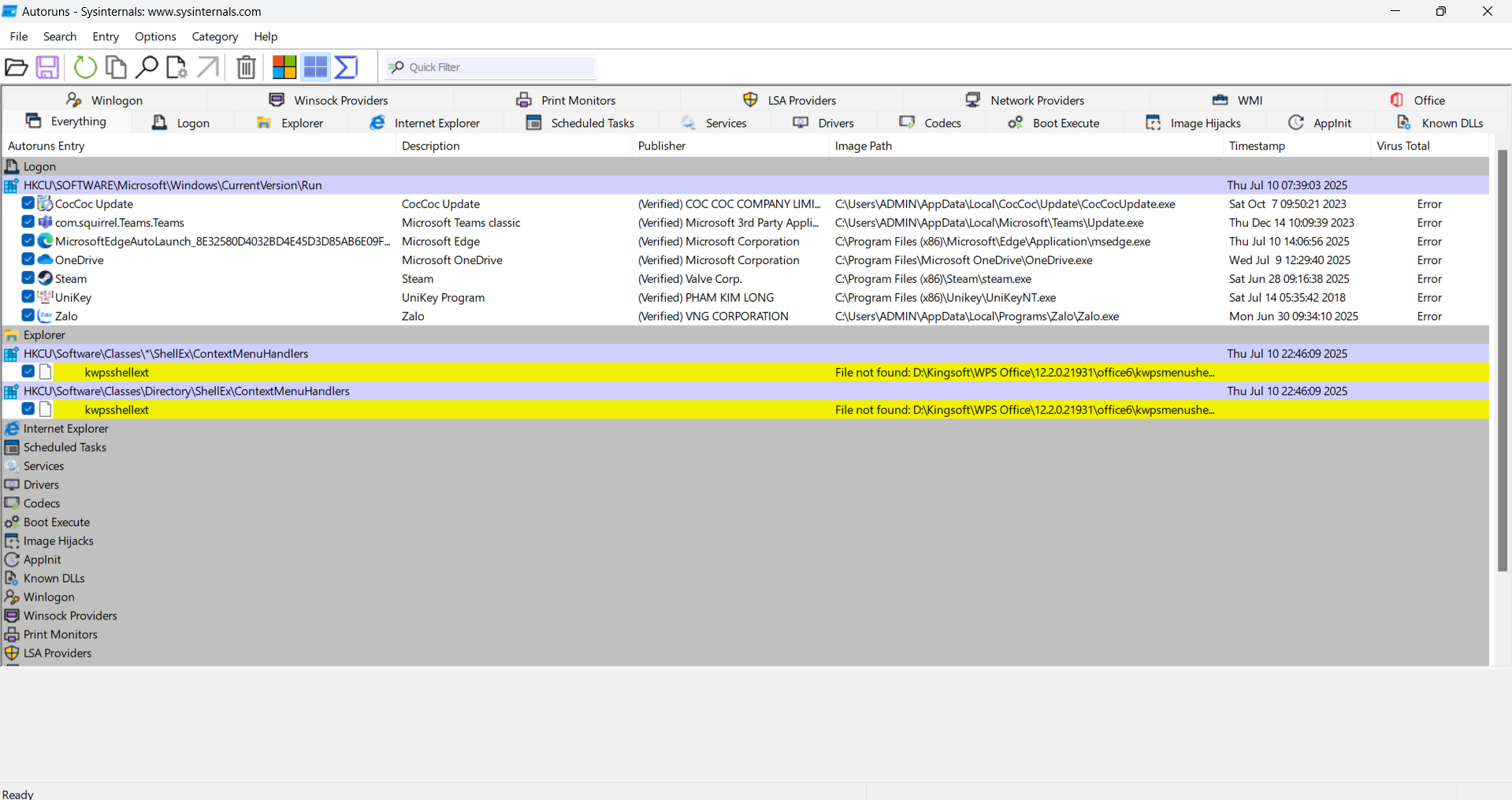


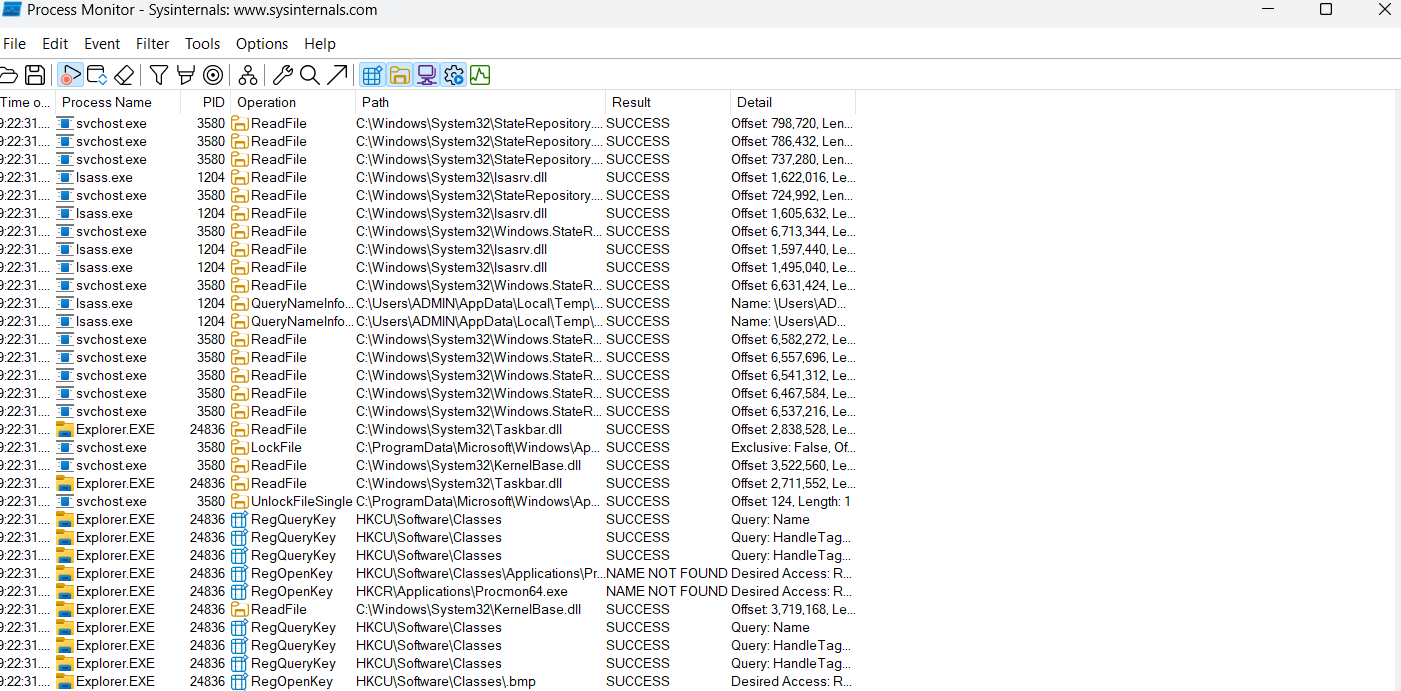


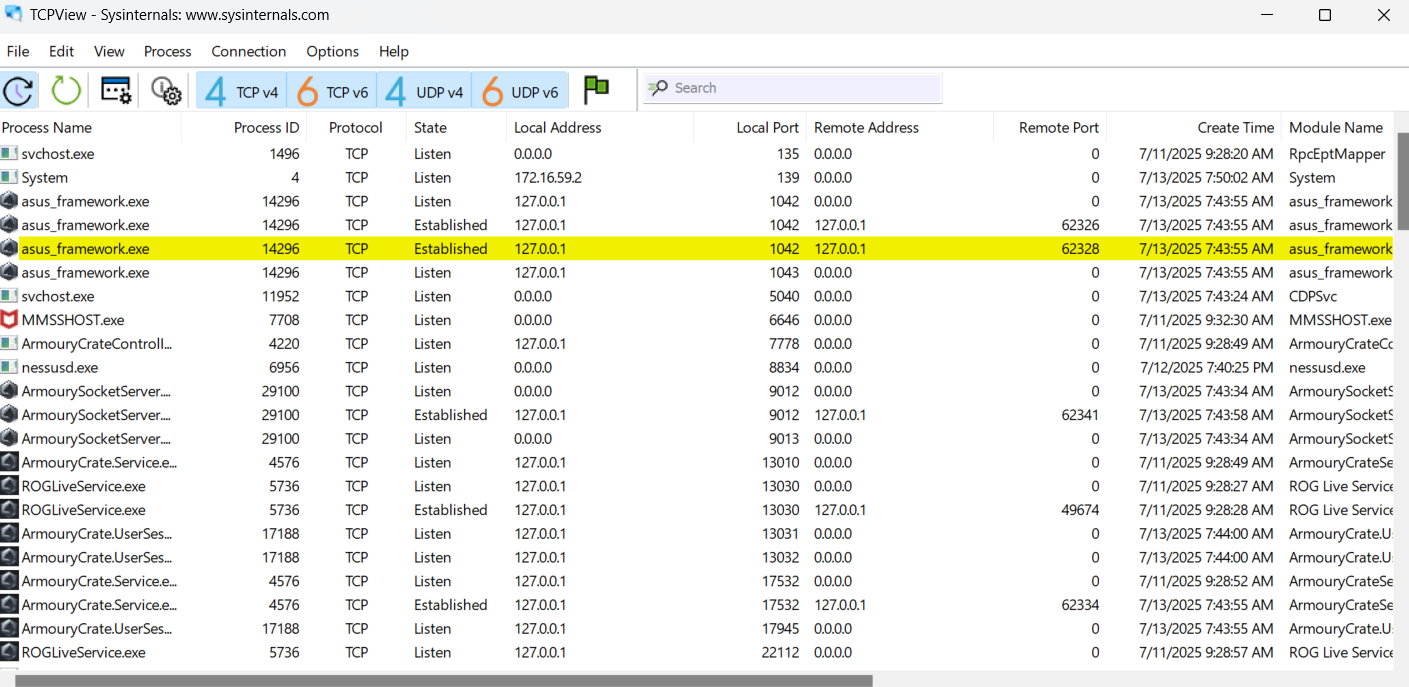
| **STT** | **Điểm yếu bảo mật** | **Mô tả chi tiết** | **Mức độ nghiêm trọng** | **Công cụ sử dụng** |
| --- | --- | --- | --- | --- |
| 1 | Lộ thông tin máy chủ | Cấu hình máy chủ tiết lộ thông tin phiên bản, giúp hacker đánh giá năng lực và tìm cách tấn công | Low | URL trực tiếp |
| 2 | Mở cổng dịch vụ nguy hiểm | Phát hiện các cổng dịch vụ nguy hiểm (RDP, VPN, HTTP, HTTPS...) có thể bị khai thác | High | Nmap, Shodan, Fping |
| 3 | Tiết lộ thông tin website | Lộ công nghệ website, plugin, CMS, framework giúp hacker đánh giá lỗ hổng bảo mật | Medium | Whatweb, Builtwith, Wappalyzer |
| 4 | Dò tên miền phụ (Subdomain) | Lộ các subdomain ẩn, có thể chứa ứng dụng quản trị, dịch vụ nội bộ hoặc file backup | Medium | Subfinder, URLScan.io, Project Discovery Subfinder |
| 5 | Tiết lộ thông tin lịch sử | Hacker khai thác dữ liệu lịch sử website qua Wayback Machine, Ahmia.fi... | Low | Wayback Machine, Ahmia.fi |
| 6 | Lộ thông tin Email/OSINT | Thu thập email, thông tin nhân sự, vị trí địa lý qua công cụ OSINT | Medium | Google Dork, Snov.io, GHunt, Mr Holmes, OSINT Framework |

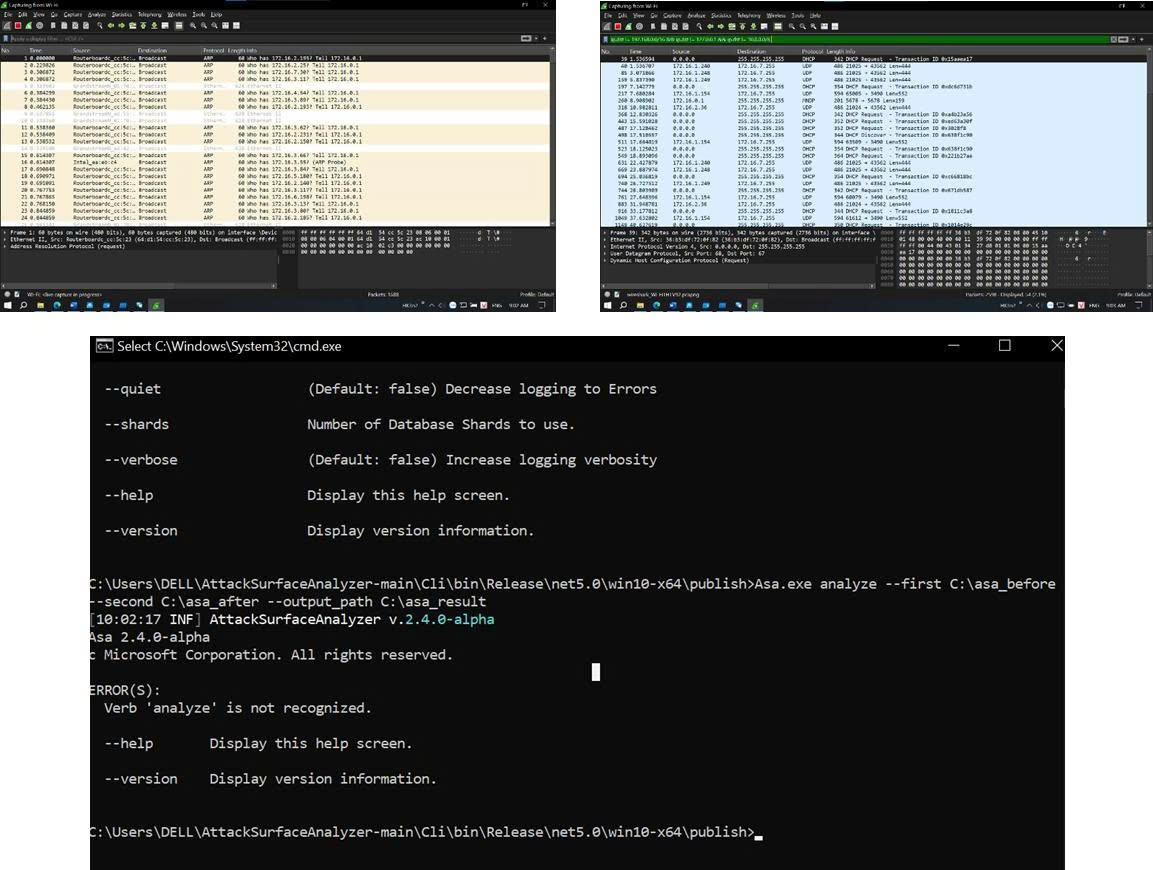












Lab4

