1. Bu zararlı yazılıma verilen ad nedir?
2. Bu zararlı yazılımın amacı nedir?
3. Zararlı yazılım için oluşturulabilecek ağ tabanlı imza nedir?
4. Bu zararlı yazılımın bir sisteme bulaştığını nasıl anlayabiliriz?
5. Zararlı yazılımın başka sistemlere yayılmasını önlemek için nasıl bir yol izlenebilir?
6. Bu zararlı yazılım ile ilgili Genel Müdür’e bir rapor verilmesi gerekiyor. Teknik ayrıntıları asgari düzeyde tutarak aşağıdaki noktaları özetleyiniz;
   1. Zararlı yazılım nasıl bulaşmış?
   2. Zararlı yazılım neler çalmış?
   3. Yapılan onbinlerce liralık güvenlik yatırımları (Firewall, antivirüs, vb.) bu zararlı yazılımın bulaşmasını neden engelleyememiş?

Zararlı yazılımın analizi eğitim sırasında gördüğümüz aşağıdaki araçlarla yapıp (6. Soruda istenen yönetici özetine ek olarak) teknik bir rapor (zararlı yazılımın faaliyetleri, iletişim kurduğu alanadları, vb.) hazırlayınız.

Raporu okuyan başka bir SOME üyesinin bu zararlı yazılımın amacının ne olduğunun, nelere dikkat etmesi gerektiğini, bu zararlının bulaştığı bilgisayarları nasıl tespit edebileceğini anlayabilmesini sağladığınızdan emin olun.

* Strings (Kali üzerinde hazır yüklü)
* PEid (<https://www.aldeid.com/wiki/PEiD>)
* Dependency Walker (<http://www.dependencywalker.com/>)
* Process Explorer (<https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer>)
* Process Monitor (<https://docs.microsoft.com/en-us/sysinternals/downloads/procmon>)