المشروع كالتالي:

1: نطور فيروسًا يجمع الملفات والصور وأي شيء مهم من جهاز الضحية ويرسلها إلى جهاز آخر

يجمع من مسار محدد مثلاً

ملفات سطح المكتب

2: يلتقط المحقق صورة للذاكرة العشوائية لجهاز الضحية

RAM

Network

3: يحلل المحقق الصورة ويكتشف البيانات المأخوذة

4: معرفة اسم الفيروس المستخدم والاتصال الذي كان الجاني يجريه

5: نتمكن من إيقاف الفيروس

6: معرفة من كان يستخرج البيانات من جهاز الضحية وايش اخذ من بيانات

7: كتابة تقرير عن الحادثة