Case Study 6: Virus Attack

First Commercial Bank is a private bank which caters to 600o customers in Rochester, New York.

A virus called “MaMia.w32” hit the computers at First Commercial Bank. This virus infected the bank’s 200 computers. As a result, all the data was lost. The “MaMia.w32” virus formatted the entire hard disk upon infection.

All the computers in the bank are backed up every Sunday at 7.00 P.M. The virus infected on Saturday 2.00 P.M. So one week of work was lost.

Nick Madison in a frantic voice calls your Super Computer Forensics Company, which is located in Atlanta, GA and requests your professional service.

Nick asks you to recover the data from all the 200 computers infected by the virus. You tell Nick that you will need 10 computer forensics professionals to assist you with this investigation and will cost him lots of money, to which Nick says, “Money is not an issue as long as the data is recovered successfully”..

How will you investigate this incident?

Answers:

1. Imaging 200 computers; assuming the capacity of each hard disk is 100GB, you will need to make at least 2 bit stream copies of the original hard disk. (It is a forensics rule).
2. That means 2 x 100 GB x 200 Computers = 40,000 GB of data storage space to begin investigation.
3. Your forensic laboratory does not have a storage capacity of such a large size.
4. You call freelance computer forensics investigators in Rochester if they would like to join with you in the investigation. They agree after negotiating a high per day fees with you. 10 of the freelances join you for this investigation.
5. You and your forensics team visit the First Commercial Bank and remove the virus infected hard disks from the computers.
6. Place the hard disks carefully in anti-static bags and transport it to the forensics laboratory.
7. Your forensics laboratory is piled up with the hard disks of the First Commercial Bank.
8. You rent 50,000 GB EMC rack servers from the Disaster Recovery Centre Inc. in New York City.
9. The Disaster Recovery Centre Inc. sends you the huge racks in a special truck to your forensics laboratory.
10. You and your team of forensics investigators make a bit-stream image of the hard disks using tools such as FTK and Encase.
11. You also generate MD5 or SHA1 hashes of the bit stream images.
12. You prepare the chain of custody and store the 200 original hard disks in a secure location. You would be investigating the bit stream image copies.
13. You take a single hard disk image to study the possibility of recovering the data.
14. You use R Drive to load the image to a free partition on the local computer.
15. The loaded image shows as D: drive of 70 GB.
16. You scan the D: drive and notice that all the files have been deleted and the drive is not readable.
17. You install the “Handy Recovery” utility and view the deleted partitions from the D: drive. It shows that 5 partitions have been deleted.
18. You restore all the 5 partitions along with the deleted files to your local C: drive. You also note that all recovered files are intact and in good condition.

19. The reason why you could successfully restore the data was that the deleted data was not over written with other data.
20. You follow the same procedure to successfully recover the data in the remaining 199 hard disks.
21. You call Nick and tell him that your team was successful in restoring the data and how he would like the recovered data to be delivered to him.
22. Nick tells you to format the existing hard disk and load the recovered data on each hard disk.
23. Your team produces a forensics report and delivers the report along with the 200 hard disks to Nick.
24. You disk wipe the data on the rented EMC storage servers and return the servers to the Data Recovery Centre Inc.
25. You charge First Commercial Bank for your professional services as follows:
    a. Your team consists of 10 investigators plus you. In total you are an 11 member team.
    b. Your team works 8 hours a day for 4 days.
    c. Your team charges $200 per hour.
    d. The rental charges for EMC storage servers costs you $ 8000 for 4 days.
    e. Transportation charges for the rented EMC rack servers, hotel charges, car rental, and airfare for travel to New York and back costs you $ 20,000.
    f. Your professional fees for the forensics investigation service costs $18,000.
    g. Total Cost = 8 x 200 x 10 x 4 + 8000 + 20000 + 10000 = $110,000.
26. You invoice First Commercial Bank for your service rendered.