[an error occurred while processing this directive]

Home

About The Project

Research Alliance

Challenges

Presentations

Whitepapers

Tools

Our Book

Funding/Donations

Mirrors

Search

Scan of the Month

Scan 24

This month's challenge is a little different. Sponsored by the folks from Digital Forensic Research WorkShop, they have created a fictional situation, where your job is to analyze forensic evidence. All submissions are due no later then 23:00 EST, Friday, 25 October. Results will be released Friday, 01 November.

Skill Level: *Intermediate*

The Challenge:
The folks from Digital Forensic Research WorkShop have created a unique challenge for you. Your mission is to analyze a recovered floppy and answer the questions below. What makes this challenge unique, you will need to read the police report before continuing your challenge. Just like an investigation in the real world, you will have some background information and some evidence, but its up to you and your technical skills to dig up the answers. Below is the dd image of the recovered floppy. This is the image that will provide you the answers, providing you can 'extract' the data.

Download:
image.zip MD5 = b676147f63923e1f428131d59b1d6a72 (image.zip)

Make sure you check the MD5 checksum of your download *before* you unzip it.

Questions
You can find all the criteria for judging and rules at the SotM main page.

1. Who is Joe Jacob's supplier of marijuana and what is the address listed for the supplier?

2. What crucial data is available within the coverpage.jpg file and why is this data crucial?
3. What (if any) other high schools besides Smith Hill does Joe Jacobs frequent?
4. For each file, what processes were taken by the suspect to mask them from others?
5. What processes did you (the investigator) use to successfully examine the entire contents of each file?

   Bonus Question:

6. What Microsoft program was used to create the Cover Page file. What is your proof (Proof is the key to getting this question right, not just making a guess).

Some URLs to help you out

- Forensic Tools.
- Scan of the Month 15.
- Honeynet Forensic Challenge.

The Results:
This months challenge questions, judging and team write-up are done by the Digital Forensic Research WorkShop. Also, Honeynet member Brian Carrier detailed how he analyzed the floppy image using his OpenSource forensics tool, TASK.

Daniel J. Kalil, DFRWS
Brian Carrier

Writeup from the Security Community
We received over 90 submissions for the challenge, by far the most we have ever received! After judging all of them, we decided to post only the Top 30. We are hitting the point where we can no longer post ever single entry as we are running out of resources. This will become a new policy for SotM challenges, whenever we receive more then 30 submissions, only the top 30 will be posted. We hope you folks will understand.

TOP 30

1. Dennis Ruck

2. Fox-IT Management Team

3. Redhive Labs

4. Eloy Paris

5. Nick DeBaggis

6. Chan Chun Fai
7. Erik Cabetas
8. Tyler Hudak
9. CERIAS
10. NCSU
11. NST-NDCA
12. Yoann Le Corvic
13. Peter Mc Laughlin
14. Charley Pfaff
15. Jason Scheuerman
16. Marc Bayerkohler
17. Daniel Sedory
18. Bill Moylan
19. Bob Mathews
20. Fox-IT Technical Team
21. Nicola Gatta
22. Jeff Craig
23. Josh Berghouse
24. Albert Bendicho
25. Jeff Wichman
26. Derek Marcotte
27. John Henry
28. Artjom Grudnitsky
29. Azzazzin
30. Barbara Pease

▲ Back to Top