SANS Digital Forensics and Incident Response Blog

04 Sep 2014

Super Sunday Funday Forensic Challenge

0 comments Posted by SANS Institute
Filed under Computer Forensics, SANS Institute, Specials, Training

The Challenge: Starting September 4, 2014 on the Hacking Exposed Computer Forensics Blog the first forensicimage will be available for download. Your goal is to solve the questionwith the first forensic image and email it to dcowen@g-cpartners.com.

The Challenge:

The first forensic image is available for download. Your goal is to solve the question with the first forensic image located at:https://mega.co.nz/#!qoxgGYCY!1jM32pncF0wE-TROhaXFI07hZbu5AfZ1BJE-p8tm1mo

and email the answer to the following questionsto:dcowen@g-cpartners.com.

- What was used to wipe this drive?
- What special options were given?
- What file was wiped from this drive?

On receiving a correct answer you will be notified that you have enteredstage 2 and that another question and image will be sent to you. Thereare 5 stages and the player who makes it the farthest with the mostcorrect answer will win!

The Rules:
1. This will be a multi stage contest lasting two weeks
2. Final answers must be in by Sept 15th
3. 9/05/14 The first question will be posted
4. New questions will be given to those who answer the firstquestion correctly
5. You can start the contest at any point leading up to Sept 15th,there is no penalty for starting late
6. All submissions must be sent todcowen@g-cpartners.com, do notpost answers in the comments
7. In order for an anonymous winner to receive a prize they mustgive their name to me, but i will not release it in a blog post

The Prize:
A free vLive DFIR Online LIVE Course from SANS a prize worth $5,000, you can choosefrom the following:

FOR408: Windows Forensic Analysis
Oct 6, 2014 - Nov 12, 2014
w/ Mike Pilkington & Ovie Carroll

FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques
Oct 13, 2014 - Nov 19, 2014
w/ Lenny Zeltser & Jake Williams

FOR508: Advanced Incident Response
Oct 14, 2014 - Nov 20, 2014
w/ Jake Williams & Alissa Torres

RSS

Search

Categories

- Advanced Persistent Threat (31)
- apt (21)
- artifact analysis (81)
- Book Reviews (5)
- Browser Forensics (33)
- Career (1)
- Case Leads (118)
- Certification and License (9)
- Challenge (9)
- Cloud Forensics (2)
- Community SANS Events (3)
- Computer Forensic Hero (2)
- Computer Forensics (613)
- Computer Forensics and IR Summit (26)
- Cyber Kill Chain (4)
- Cyber Threat Intelligence (11)
- DFIR Summit (8)
- Digital Forensic Law (50)
- Drive Encryption (18)
- eDiscovery (50)
- Email Investigations (18)
- Ethics (9)
- Evidence Acquisition (114)
- Evidence Analysis (192)
- Getting Started (25)
- HeartBleed (1)
- Incident Response (175)
- Linux IR (28)
- Malware Analysis (103)
- Memory Analysis (59)
- Mobile Device Forensics (56)
- Network Forensics (51)
- Network Forensics (6)
- Registry Analysis (26)
- REMnux (3)
- Reporting (21)
- Reverse Engineering (51)
- SANS Institute (50)
- SANS Survey (1)
- SIFT Workstation (15)
- smartphone (1)

Permalink | Comments RSS Feed - Post a comment | Trackback URL

Post a Comment

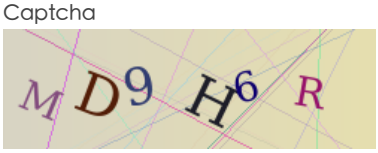
*Name

*Email

Website

*Comment

Captcha



*Response

Post Comment

* Indicates a required field.

- Specials (22)
- Threat Hunting (2)
- Timeline Analysis (22)
- Training (37)
- Uncategorized (4)
- USB Device Analysis (13)
- Volatility (2)
- Windows IR (80)
- Windows Memory Forensics (7)
- Write Blockers (13)

Recent Posts

- SANS CTI Summit & Training Twitter Contest
- DFIR Summit 2016 - Call for Papers Now Open
- SANS ThreatConnect DFIR Threat Intelligence Sharing Community Announced
- Using ProcDOT Plugins to Examine PCAP Files When Analyzing Malware
- Threat Hunting and Incident Response Summit - CFP - Closing 12 Oct

Recent Comments

Popular Posts

Archives

Select Month

Links

- Log in
- Entries RSS
- Comments RSS

Latest Blog Posts

SANS CTI Summit & Training Twitter Contest
January 08, 2016 - 12:12 PM

DFIR Summit 2016 - Call for Papers Now Open
November 16, 2015 - 8:19 PM

SANS ThreatConnect DFIR Threat Intelligence Sharing Community Announced
October 07, 2015 - 2:08 PM

Latest Tweets @sansforensics

In one week, join @alexcpsec for his webcast "Data Driven Th [...]
January 12, 2016 - 9:03 PM

It starts NOW! Intelligent Intelligence w/ @DavidJBianco En [...]
January 12, 2016 - 8:03 PM

15 minutes to register for the @DavidJBianco webcast on secr [...]
January 12, 2016 - 7:46 PM

Latest Papers

Investigative Forensic Workflow-based Case Study for Vectra and Cyphort
By Jennifer Mellone

On the x86 Representation of Object Oriented Programming Concepts for Reverse Engineers
By Jason Batchelor

On the x86 Representation of Object Oriented Programming Concepts for Reverse Engineers
By Jason Batchelor

"This is awesome! We're seeing details that most people don't even know exist."
- John Wright, Info Tech, Inc.

"Forensics is a lot more than just imaging a drive."
- Joseph Fresch, Guaranty Bank

"Rob Lee is a master of the subject matter. The material is presented in a way that is understandable. Rob is also charismatic enough to make the course enjoyable."
- Erik Ketlet, JP Morgan Chase