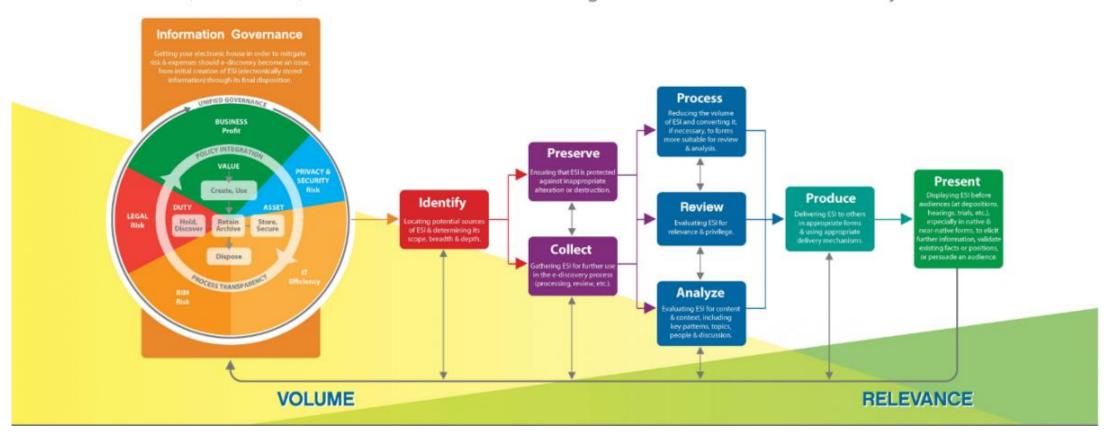
Forensic Investigations

ISC2 – October 2020 Incident Response FORENSIC & CYBER

Electronic Discovery Reference Model

Standards, Guidelines, and Practical Resources for Legal Professionals and E-Discovery Practitioners





Windows Forensic Analysis —— P O S T E R —

You Can't Protect What You Don't Know About

digital-forensics.sans.org



Windows Artifact Analysis: Evidence of...

Windows Time Rules

\$STANDARD_INFORMATION The state of the s

File Download

Program Execution

Deleted File or File Knowledge

XP Search - ACMRU

Search - WordWheelQuery

IE|Edge file://

Last-Visited MRU



die militation de la constitución de la constitució







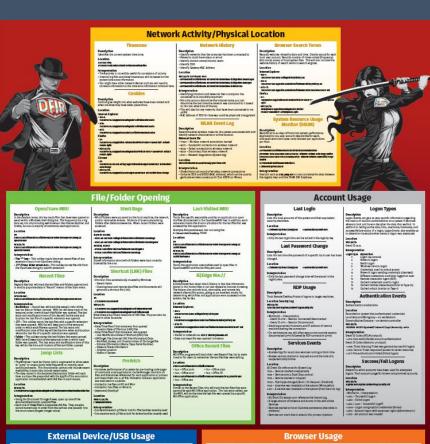












External	Dev	rice/USB	Us	age
Identification	1	PnD Events	1	Drive I

First/Last Times

ocation statutes lugand Floy lag Files

Spring relating from reduced to the control of the

Volume Name
Description
Description and set of the 200
Description and the set of the 200
Description and the set of the 200
Description and the set of the 200
Location and the place of the set of t

Shortcut (LNK) Files

Description

- Shortcut (LNK) Files

Description

- Short Land (LNK) Files

Description

- Short Land

- S

Hardware Analysis and the State of Stat

Description

Characteristics and any amountment and is contained.

Description

Description and any amountment and is contained.

Description and any amountment and is contained.

Description and any amountment amountmen

The New York Times

Wednesday, October 21, 2020

Today's Paper

U.S. Politics N.Y. Magazine T Magazine Video Business Opinion Tech Science Health Sports Arts Books Style Food Travel Real Estate S&P 500 -0.22% ↓ Your Thursday Briefing Listen to the Modern Love Podcast The Book Review Podcast 21° 15° President Trump's business pursuits Alan Mikhail and Benjamin Lorr The unexpected aftermath of a Dow -0.35% ↓ in China. discuss their new books. breakup. Auckland, New Zealand -0.28% ↓ Nasdag

Pope Francis, in Shift for Church, Voices Support for Same-Sex Civil Unions

- The comments, made in a new documentary, are the strongest yet from a pontificate that has taken a more tolerant and inclusive tone.
- "What we have to create is a civil union law," Francis said amid remarks in which he reiterated his support for gay people as children of God.



Pope Francis speaking during the weekly general audience at the Vatican on Wednesday.

Opinion

Farhad Manjoo

I Spoke to a Scholar of Conspiracy Theories and I'm Scared for Us

In 2020, any hint of optimism feels dangerously naïve.

Nicholas Kristof

She's Evangelical, 'Pro-Life' and Voting for Biden

Billy Graham's granddaughter says, "This president doesn't represent our faith."



Ashley Fetters

Your Work Friends Knew

Thomas L. Friedman





y Follow @GaryChappellDE

Mobile journalism masterclass

A six-week course starting 2 November



Subscribe to our newsletter for

PressGo, PressQ, Freelance, JTweeps , Newsrewired , Home , Jobs , Training , Journalists on Twitter Jobs board Journalists on Twitter » View all **20** job vacancies Sector Added | Followers | Name | Handle | Last Tweet | ^ Job of the week 1 to 15 of 9895 publisher: publication: Editor - London RoyalReporter full search: Reorg, a provider of financial information and Name: Richard Palmer analysis on distressed and high yield debt, is Sector: Newspaper Search looking for an experienced editor to share the Publication: Daily Express Job title: Royal correspondent lead in our London office Followers: 117,260 > View all Featured jobs » Request inclusion » Digital news curator - upday » Finance/business writer part-time - Confidential -VC-backed FinTech Wiew full details » Freelance journalist - Newslead » Investment reporter - Citywire >> Editor - 3 days per week - Social Spider CIC GaryChappellDE Name: Gary Chappell Go to the jobs board Sector: Newspaper **Publication:** Daily Express Job title: Assistant content editor, sport Followers: 1,258 Free daily newsletter





Given the care, given the attention to detail and the fact that they did it without malice, they did it without any ad hominem approach.

Bill Hodge, Auckland University

Case Study – Cloud Ransomware Attack

Day 0	Day 1	Day 2	Days 3-7	Days 8-10	
Preparation	Identification, Containment	Containment, Eradication	Eradication, Recovery	Recovery	
Cyber risk assessment Critical assets identified, protected and monitored Incident response plan Public relations statements Tabletop exercise simulation	Ransomware identified on cloud-based servers Initiate incident response plan Determine data was 'Test', so plan to rebuild servers Organisation unable to determine what the infected data contained, whether PII/PCI was present or whether data had been copied Forensic technology experts engaged War Room Convenes	Cloud server data copied for examination Log files and other forensic artefacts copied All ransomware files erased Cloud servers rebuilt for BAU Examination of forensic data locates evidence of persistent access to corporate email system and 'Man in the Middle' attacks due to actual data being used in 'Test' instead of 'Masked' data Ongoing War Room	Plan to communicate with parties affected by email attack Liaison with Legal, HR, PR, Privacy Forensic report issued on the extent of personally identifiable information and email data being breached Data breach notifications issued Testing all systems for BAU Improved monitoring Ongoing War Room	Post Incident Review Cause – combination of test data not being masked and weak monitoring systems Update incident response plan Plan to implement stronger two-factor authentication for remote email access Enforce final contact of a 'phone call' with clients to identify possible 'Man in the Middle' vulnerabilities Final War Room Debrief	



Thank you

Campbell McKenzie

0800 WITNESS

021 779 310

campbell@incidentresponse.co.nz

incidentresponse.co.nz

We help you Prepare, Respond and Recover from Forensic and Cyber Incidents