**Trends in Digital Forensics in 2020**

The field of Digital Forensics has grown and matured rapidly in the past two decades. It has given rise to special disciplines where professionals can apply the skills of digital forensics. A critical demonstration of this is DFIR short for Digital Forensics and Incident Response which applies forensics to cyber security incidents such as malware attacks and data breach.

The threats in field of cyber security however continue to grow and the cost of these incidents are more weighty than ever. Consider these sobering statistics:

Security breaches have increased substantially by 11% since 2018 and 67% since 2014.

Hackers attack estimably every 39 seconds; on average 2,244 times a day.

The average identification time of a breach in 2019 was 206 days.

Presently, the average lifecycle of a breach is 314 days, from breach to containment.

While dealing with data breaches is a critical challenge for private industries, it is all the more problematic for the public sector as they often lack resources to ascend an adequate defence against attacks and to carefully conduct DFIR investigations subsequent to it.

One popular and common example is ransomware. “Ransomware is a textbook case of extortion and it’s happening more and more frequently to local governments,” as reported by Governing Magazine in October 2019. “This isn’t happening by mistake, attackers are actively targeting governments because they may not have the cybersecurity protections in place due to outdated solutions or budgetary constraints.” These bold attacks are becoming increasingly costly to government agencies. A study in 2019 by Coveware found that the average ransomware payment from a government rose to $338,700, compared to $36,295 for private-sector victims.

Other examples include malware attacks and theft of government records that can be monetized by crime rings in both India and abroad. Even cybersecurity attacks that do not escalate to the point of extortion, hack into the information systems can paralyse the entire organisation.

Here are five DFIR trends to watch out for in 2020:

1. Use of advanced technology by bad actors

Cybercriminals are growing more sophisticated in their use of technologies that allow them to hide their conduct better than ever. Viruses are increasingly planted through virtual sessions and other remote techniques that make individual workers unwitting participants in cyber intrusions that wreak havoc on government networks. Public sector DFIR professionals are preparing for the nefarious use of technologies in 2020 that we can’t even imagine yet.

2. Growth of mobile device capabilities

Mobile devices can now perform virtually any computing task that a laptop or a desktop can. This means that cybercrime teams no longer need a secluded “war room” for attack plan. Any bad actors can launch cyberattacks with the phones in their pockets.

3. Targeting data in the cloud

All sorts of personal data is now preferably being stored in the cloud, from personal financial information and confidential legal documents to protected medical records and private government communications. A 2019 report from Skybox Security found that data security threats to prominent cloud service providers is rising but so far the number of successful attacks has been extremely limited. DFIR professionals in the public sector anticipate that cloud storage will become an even more intense battleground in 2020 between cyber criminals and law enforcement agencies.

4. Increased collaboration between investigators

DFIR workflows tend to be quite different in the public and private sectors, which is the result of unequal levels of available resources and much different budget allocation timeframes. However, our customers in both environments are dealing with similar cybersecurity threats and DFIR challenges. The experts we spoke to predicted that the industry will see more collaboration next year between digital forensics professionals working for government agencies and corporations, as they try to help each other deal with a series of common challenges.

5. Greater focus on incident response

Digital Forensics (DF) is well known as an important discipline for law enforcement investigations of various types, but many experts believe there is not enough attention placed on the Incident Response (IR) piece of the equation. A good IR plan helps government teams map their data perimeter in advance of a possible attack and then inform their investigation in the crucial early hours after an incident by helping them find where the breached data resides as quickly as possible. Public sector DFIR professionals believe that we will see more emphasis on IR in 2020 and beyond.

Digital forensics professionals who work in the public sector need to have access to a full range of advanced software products in their toolkits if they are going to be prepared to conduct effective DFIR investigations in 2020. AccessData has been an industry leader in developing and delivering tools that assist government agencies with post-breach digital forensics investigations and incident response.

Earlier this year, we introduced a new version of AD Enterprise, our software for managing internal forensic investigations and post-breach analysis, which included first-to-market integration with cybersecurity platforms to automate the early stages of data collection. AD Enterprise is a powerful tool for post-breach analysis, offering live data preview at the endpoint. It can be deployed in the cloud quickly and securely, which is an attractive option for many public sector clients that need a tool for post-breach analysis but lack the time and resources to spin up their own technology infrastructure when they’re in the chaos of a cyber incident. AD Enterprise can be up and running within a matter of hours.

We have extended this focus on innovation with post-breach software tools by creating the first API that helps to automate the crucial early stages of data collection and forensics captures immediately following a cyber incident. With the AccessData API, AD Enterprise can connect with any government agency’s cybersecurity software platform of choice. If the cybersecurity software detects an attack, it triggers an alert via the API that is received by AD Enterprise, which initiates a collection job within moments at a designated endpoint or affected asset. This saves precious time in the initial stages of the incident response by preserving data related to the root cause of the breach, as well as preservation of critical data and important time sensitive forensics.

Cybersecurity threats continue to evolve in both number and sophistication, a trend that experts concede will continue in the year ahead. But access to the right information, collaboration with other professionals in the DFIR community and use of leading-edge software tools can help public sector digital forensics professionals be better prepared for attacks and accelerate their incident response efforts.

**Statistical Tools for Digital Forensics**

Some of the proposed approaches by which an image can be authenticated are Digital watermarking,embedded signatures, erasable fragile watermarks , semi-fragile watermarks, robust tell-tale watermarks, and self-embedding watermarks. All of these approaches work on some assumptions which are not yet clear whether they are reasonable assumptions or not. Due to non reliability of the above mentioned approaches, the author describes a class of statistical techniques for detecting traces of digital tampering in the absence of any watermark or signature. These approaches work on the assumption that although digital forgeries may leave no visual clues of having been tampered with, they may, nevertheless,alter the underlying statistics of an image.

# **Re-sampling**

In order to create a convincing match of image, it is often necessary to re-size, rotate, or stretch the images, or portions of them. These manipulations require re-sampling an image onto a new sampling lattice using some form of interpolation. Although the re-sampling of an image is often imperceptible, specific correlations are introduced in the re-sampled image. When detected, these correlations represent evidence of tampering. Author uses these correlations and proposed an algorithm for detecting any sign of tampering in any portion of an image.Author describe the form of these correlations, and propose an algorithm for detecting them in any portion of an image. In this algorithm, depending on the re-sampling rate, the re-sampling process will introduce correlations of varying degrees between neighboring samples. First up-sampling of the signal is done ,then the interpolation, and last down-sampling of the signal and periodicity is calculated. Based on the periodicity of the re-sampling matrix, the sampled signal will have the same correlations to their neighbors. The specific form of the correlations can be determined by finding the neighborhood size,N,and the set of weights,α, that satisfy:ai=∑Nk=−Nαkai+k, where ai is the ith row of the re-sampling matrix and i is a numerical value such as 3,7,11 etc.

The periodic pattern introduced by re-sampling depends on the sampling rate. As a result, it is possible to

not only uncover traces of re-sampling, but to also estimate the amount of re-sampling. It is not

possible,however, to uniquely determine the specific amount of re-sampling as there are re-sampling parameters that yield similar periodic patterns.There is also a range of re-sampling rates that will not introduce periodic correlations.

JPEG standard specified two compression schemes:a lossless predictive scheme and a lossy scheme based on the Discrete CosineTransform (DCT).

The encoding of an JPEG image involves three basic steps:

1. Discrete Cosine Transform (DCT): An image is divided into 8×8 blocks in raster scan order (left to right, top to bottom), shifted from unsigned to signed integers, and each block’s DCT computed.

2. Quantization: The DCT coefficients obtained in the previous step are uni-ormly quantized, i.e., divided by a quantization step and rounded off to the nearest integer. Since quantization is a non-invertible operation this step represents the main source of information loss.

3. Entropy Encoding: This step involves lossless entropy compression that trans-forms the quantized DCT coefficients into a stream of compressed data. The most frequently used procedure is Huffman coding, although arithmetic cod-ing is also supported.

# **Double JPEG Compression**

Decoding of an image involves the inverse of these steps.The histograms of the DCT coefficients are computed. If these histograms contain periodic patterns, then the image is very likely to have been double compressed. The periodic patterns introduced by double JPEG compression depend on the quality parameters. As a result, it is possible to detect not only if an image has been double compressed, but also the compression qualities that have been used. The second parameter can be found from the quantization table stored in the JPEG file. The first parameter can be inferred from the location of the frequency peaks in the Fourier transforms of the DCT coefficient histograms. If a JPEG image is double compressed it is very likely that the image is tampered.

# **Luminance Non-linearities**

The quality of digital images can be improved using luminance non-linearity , parameters are held constant and dynamically chosen.The presence of several distinct non-linearities in an image is a sign of possible tampering. local non-linearities can be applied in the composite image in order to create a convincing luminance match.

Previously a technique was proposed to estimate parametric models of geometric and luminance nonlinearities from digital images.That technique exploits a fact in the Fourier domain.Some tools are used from poly spectral analysis. Same technique can be employed if an image contains multiple nonlinearities.

Pointwise non-linear transformations introduce specific correlations in the frequency domain. Consider a one-dimensional discrete signal composed of a sum of two sinusoids having different phases and

amplitudes: x[t] = a1 cos(ω1t + φ1) + a2 cos(ω2t + φ2). Consider also a generic nonlinear function g(·) and its Taylor series expansion where the various scalar constants and terms of degree higher than two are ignored: g(u) ≈ u + u.2 . The non-linearly transformed signal takes the form: g(x[t]) = −0.5(a 2 1 + a 2 2 ) + a1 cos(ω1t + φ1) + a2 cos(ω2t + φ2) + 0.5a 2 1 cos(2ω1t + 2φ1) +0.5a 2 2 cos(2ω2t + 2φ2) + a1a2 cos((ω1 + ω2)t + (φ1 + φ2)) + a1a2 cos((ω1 − ω2)t + (φ1 − φ2)). (19) .These type of correlations generalize to any type of underlying signal and pointwise nonlinearity. Let X(ω) denote the Fourier transform of x[t]: X(ω) = P∞ t=−∞ x[t]e −itω. The power spectrum is a commonly employed tool to estimate second order correlations: P(ω) = E{X(ω)X∗ (ω)}, where E{·} is the expected value operator, and ∗ denotes the complex conjugate. For example, the bispectrum can be employed to estimate third order correlations: B(ω1, ω2) = E{X(ω1)X(ω2)X∗ (ω1 + ω2)}.Compute the Fourier transform of each segment k: Xk(ω), compute an average estimate of the bispectrum using the Fourier transform of individual segments Bˆ(ω1, ω2) = 1/N PN k=1 Xk(ω1)Xk(ω2)X∗ k (ω1 + ω2). The bispectrum has the undesired property that its value at bi-frequency (ω1, ω2) depends on P(ω1), P(ω2), and P(ω1 + ω2). For analysis purposes, To this end, we employ the bicoherence [13] (a normalized bispectrum), defined as: b(ω1, ω2) = |B(ω1, ω2)| (E{|X(ω1)X(ω2)| 2}E{|X(ω1 + ω2)| 2}) 1/2

It is fairly straightforward to show using the Schwarz inequality 3 that the bicoherence is guaranteed to take values in [0, 1]. Just like the bispectrum, the bicoherence can be estimated as:

ˆb(ω1, ω2) = 1 K | P k Xk(ω1)Xk(ω2)X∗ k (ω1 + ω2)| 1 K P k |Xk(ω1)Xk(ω2)| 2 1 K P k |Xk(ω1 + ω2)|

2

# **Signal to Noise Ratio**

Digital images have noise introduced either by the imaging process or digital compression. If two images with different noise levels are spliced together, or if small amounts of noise are locally added to conceal traces of tampering, then variations in the signal to noise ratio (SNR) can be used as evidence of tampering We begin by assuming an additive noise model: y[t] = x[t] + w[t], where x[t] is the uncorrupted signal with variance S and w[t] is the noise with variance N.

# **Conclusion**

Here a set of statistical tools have been described for detecting traces of digital tampering in the absence of any digital watermark or signature. We have quantified the nature of statistical correlations that result from specific forms of digital tampering, and have devised detection schemes to reveal these correlations.Also analyzing the sensitivity and robustness to counter-attack of each of the schemes outlined in this paper. There is little doubt that counter-measures will be developed to foil each of the detection schemes outlined in this paper. Our hope, however, is that as more authentication tools are developed it will become increasingly more difficult to create convincing digital forgeries. In addition, as the suite of detection tools expands we believe that it will become increasingly harder to simultaneously foil each of the detection schemes.