How Much Does Digital Forensics Services Cost?

EDUCATIONAL ARTICLE

VESTIGE
Digital Investigations

How Much Does Digital Forensics Services Cost?

As Electronic Evidence Experts who specialize specifically in digital forensics, cybersecurity, and e-discovery, we recognize that your first priority is to determine a budget for yourself or your client to make sure you can afford the digital forensic services you need. Services that can help uncover the evidence, settle the dispute or win the case.

At Vestige, we want to help, so let's get started by taking a look at some considerations for the cost of digital forensic services...

The short answer...it depends.

It's a lot like asking someone how much it costs to build a house. It involves a lot of factors. The more upfront information known about the scope of work, the tighter the estimate will be. In regard to digital forensics, ranges can be a couple thousand dollars to well over $100,000 with the typical analyses being somewhere in the $5,000 to $15,000 range, based upon factors involved.

Let's explore some of the factors that affect digital forensics pricing. You'll see that working with the 'end in mind' is key. However, don't despair if you don't know all the answers to the sample questions below when you call for digital forensic services. A qualified and experienced service like Vestige can easily guide you through the process.

- How much does the investigation team already know about the fact pattern? In essence, does the matter have a NARROW focus? (ex. We need to see if a document has been altered after this date). Or a BROAD focus? (ex. We suspect somebody did something covert in the past year.)
- Names of the parties involved? (In order to assure a quick conflict check)
- What type of investigation is expected to be performed? (ie. discovery, investigative matters, etc.)
- What kind of activities are suspected? (ie. alteration, theft (ie. data/money), deletion, defamation, anti-forensics software installed, physical damage, etc.)
- Are there particular terms being sought?
- How many devices are involved? (Don't forget – Virtualized systems are equivalent to another computer.)
- What types of devices are involved? (ie. Laptops, workstations, servers, mobile devices, tablets, cell phones, surveillance video or proprietary manufactured systems)
- Is there encryption and/or password protection installed?
- Are there multiple types of Operating Systems or virtual devices contained within the devices being analyzed? (ex. some devices have a Dual Boot OS with multiple OS versions or even different versions, such as MAC OS and Windows loaded.)

- How many users are utilizing the device(s)?
- What is the volume of activity that has occurred on the device(s)? Rarely used? Heavy usage?
- What type of output or report is required? (ie. a simple memo or finding; a report; an Expert report; Affidavit; Deposition attendance; Testimony at a hearing or trial?; etc.)
- How much data will need to be searched and analyzed? (ex. estimate in MB, GB, TB etc.)
- What is the deadline / timeframe that the analysis needs to be performed?

Other Things To Consider

There are a two approaches to pricing when it comes to digital forensic services – one is Time & Materials, the other is Flat-Fee Pricing.

Time & Materials

Many industries, including legal, are accustomed to the Time & Materials pricing model because it's how they run their own business, so it's comfortable to work with.

However, when it comes to Time & Materials billing for digital forensics – Price Shoppers Beware!

Here are three areas to watch for with digital investigation costs:

1. Low initial pricing. While this sounds great and appeals to the wallet, it is commonly caused by gross underestimation of the time a matter will actually take and is primarily a 'foot-in-the-door' tactic. There is some truth to 'You Get What You Pay For' in this business and once you sign the dotted line with an inexpensive IT guy who bought some off-the-shelf digital forensics software – regret is sure to follow.

2. Failure to ask enough questions upfront about a client's scope of work. This leads to providing an underestimated number of hours to complete the job. Once the project is in full force, it then becomes obvious more hours are required to complete the project, thus ...'hidden costs' for digital forensic services can and do begin to appear.

3. Time & Materials billers are often forced to hurry and do not perform a thorough investigation or are inexperienced in the legal and technical requirements and fail to perform the detailed forensics correctly. This can cause arrival at a partial conclusion, ignored testing of evidence which can cause totally inaccurate conclusions, and inadmissibility in court. This then causes costly time and money for back-tracking, or worse yet – the time and costs of starting over.

Today, you can expect to find hourly rates in the $200 to $450 range. A typical analysis on a single device, without any of the above complications (ie. encryption, use of forensic tools, broad scope of investigation work, etc.) will generally take 15-30 hours of work.

In our opinion, digital forensic services based on Time & Materials approach can easily inflate and end up costing considerably more than what is initially agreed upon, can produce inaccurate or inadmissible results, and is unpredictable overall.

Continued on back

Flat-Fee Pricing

While flat-fee pricing for digital forensics can seem expensive and produce temporary sticker-shock, in the long-run we believe it offers a number of benefits:

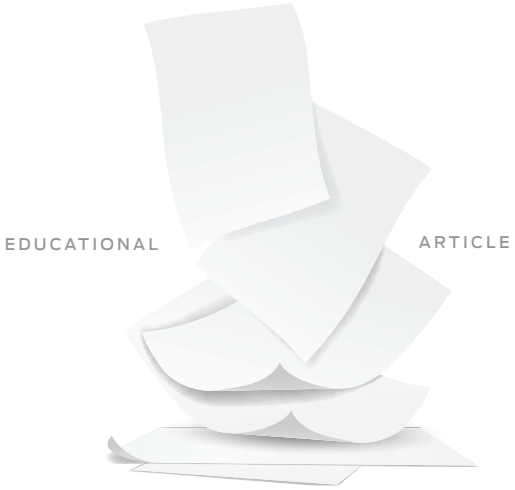
1. An upfront understanding of exact needs and expectations. Knowing a tight scope of what you're looking for helps speed along the process and aids in producing the most exact quotation – and will typically be less expensive in the long-run. Preparation to answer the aforementioned critical questions when working with a flat-fee digital forensic service provides tremendous assistance.

Look for certified digital forensic experts who will expertly and efficiently guide you through the process to determine who to find the answers from and exactly what to do each step of the way.

2. Proper Preparation, Testing & Reporting. Flat-fee pricing features the extra steps that matter — including preparation for trial at the onset. This way there is no back-tracking. This requires analysts with a thorough knowledge of both the legal, as well as the technical side of digital forensics. The focus on experience and testing cannot be underscored enough. There are many nuances that get examiners – and subsequently their clients – into trouble when opining on the evidence.

Be sure to engage a service that performs extensive testing on any digital evidence uncovered as well. Proper testing assures accurate, air-tight, and legally defensible opinions.

Finally, one needs to consider your needs as it relates to reporting. Reports should be easy to understand for the fact-finder, at the same time providing detail on the digital forensics procedures performed, verification of the tested results and any other information that aids in the resolution of the matter. ◊



.VESTIGE
Digital Investigations

For more information Contact us today
800.314.4357 or info@vestigeltd.com